



HAROLD M. EDWARDS

FERMAT'S  
LAST  
THEOREM

A GENETIC INTRODUCTION  
TO ALGEBRAIC  
NUMBER THEORY

Work on this book was supported in part by  
the James M. Vaughn, Jr., Vaughn Foundation Fund.



Г. Эдвардс

# ПОСЛЕДНЯЯ ТЕОРЕМА ФЕРМА

Генетическое введение  
В АЛГЕБРАИЧЕСКУЮ  
ТЕОРИЮ ЧИСЕЛ

Перевод с английского  
В. Л. КАЛИНИНА И А. И. СКОПИНА

под редакцией  
Б. Ф. СКУБЕНКО

ИЗДАТЕЛЬСТВО «МИР»  
МОСКВА 1980

Монография по арифметике круговых и квадратичных полей, написанная свежо и оригинально. Автор следует в своем изложении историческому ходу событий, но описывает только те идеи, которые в дальнейшем получили развитие. Поэтому он называет свой метод изложения не «историческим», а «генетическим». Каждое общее утверждение иллюстрируется конкретными примерами, что выгодно отличает книгу от других, где материал излагается на более абстрактном уровне.

В целом книга представляет несомненный интерес для математиков различных специальностей. Она может использоваться и для первоначального знакомства с предметом.

*Редакция литературы по математическим наукам*

1702030000

Э  $\frac{20203-013}{041(01)-80}$  13-80

© 1977 by Harold M. Edwards  
All rights reserved. Authorised  
translation from English language  
edition published by Springer-  
Verlag Berlin — Heidelberg —  
New York

© Перевод на русский язык, «Мир»,  
1980

## ОТ РЕДАКТОРА ПЕРЕВОДА

Пожалуй, нет ни одной математической проблемы, которая была бы столь популярна среди математиков и особенно среди математиков-любителей, как проблема Ферма (или знаменитая «Великая теорема Ферма», или «Последняя теорема Ферма»).

На русском языке имеется не так много книг, специально посвященных этой проблеме, да и книги эти из серии популярных. Однообразие проблематики, первоначально вызванная Вольфскелевской премией, вынуждает каждого пишущего о теореме Ферма быть предельно осторожным. По крайней мере написанная книга не должна вызывать сомнения в том, что ее автор не хочет иметь дело с «ферматистами».

Книга Эдвардса, предлагаемая вниманию читателей, настолько содержательна, что у любителей решать проблему Ферма примитивными методами она отобьет всякое желание дискутировать. Кстати, и книга М. М. Постникова «Теорема Ферма» (М.: Наука, 1978), не столь объемистая, как эта, наделена таким же иммунитетом.

Книга Эдвардса, как пишет сам автор в предисловии, не претендует на историчность. Это, конечно, верно, однако некоторые моменты истории математики в книге описаны весьма подробно. Достоинством книги является и то, что автор подробно излагает основы теории идеалов генетическим методом. Приятно узнавать, каким образом создавалась эта теория, какие математики в этом участвовали, какие возникали драматические, а порой и парадоксальные ситуации (например, случай с  $p = 23$ ), в итоге приведшие к гениальному открытию.

Изложение генетическим методом имеет и теневые стороны. Эдвардсу волей-неволей приходится пользоваться терминологией прошлого века, излагать доказательства теорем языком той эпохи, производить многочисленные арифметические вычисления, выпи-

сывать длинные цитаты — все это в книге соткано в единое произведение, наделенное духом нашего времени. Такое сочетание затрудняет чтение книги в оригинале и делает ее чрезвычайно сложной для перевода. Переводчики стремились сохранить свежесть и оригинальность стиля автора, и если это не всегда удалось им, то, во всяком случае, не из-за отсутствия старания. Предисловие, главы I, II, VII, VIII, IX и § 2 приложения переведены В. Л. Калининым. Главы III, IV, V, VI и § 1 приложения переведены А. И. Скопиным.

*Б. Ф. Скубенко*

## ПРЕДИСЛОВИЕ

По-видимому, многие откроют эту книгу с желанием узнать, каково современное состояние знаний о Последней теореме Ферма, и, так как сама книга не дает ответа на этот вопрос, стоит, вероятно, сказать об этом несколько слов в предисловии. Последняя теорема Ферма — это утверждение (не теорема), что уравнение  $x^n + y^n = z^n$  при  $n > 2$  не имеет целых положительных решений. Легко доказать (см. § 1.5) неразрешимость уравнения  $x^4 + y^4 = z^4$ . Поэтому исходное уравнение неразрешимо, когда  $n$  делится на 4. (Если  $n = 4k$ , то равенство  $x^n + y^n = z^n$  приводило бы к равенству  $X^4 + Y^4 = Z^4$ , где  $X = x^k$ ,  $Y = y^k$ ,  $Z = z^k$ , что невозможно.) Аналогично, если доказать неразрешимость уравнения  $x^m + y^m = z^m$  при некотором значении  $m$ , отсюда будет следовать неразрешимость исходного уравнения для любого  $n$ , делящегося на  $m$ . Поскольку каждое  $n > 2$  делится либо на 4, либо на нечетное простое число, то для доказательства Последней теоремы Ферма достаточно доказать ее для простых показателей  $n$ .

Для показателя  $n = 3$  доказать эту теорему не слишком трудно (см. гл. 2). Для показателей 5 и 7 возникают бóльшие трудности (§ 3.3 и 3.4), однако методы остаются по существу элементарными. Основное содержание книги составляет мощная теория «идеального разложения», разработанная Куммером в 40-е годы 19 века и позволившая одним махом доказать Последнюю теорему для всех простых показателей, меньших 100, кроме 37, 59 и 67. Точнее, теорема Куммера утверждает следующее. Пусть  $p$  — нечетное простое число. Тогда достаточное условие для справедливости Последней теоремы Ферма при показателе  $p$  состоит в том, что  $p$  не делит числители чисел Бернулли  $B_2, B_4, \dots, B_{p-3}$  (см. § 5.5 и 6.19). Простое число, удовлетворяющее достаточному условию Куммера, называется «регулярным».

Начиная с 1850 г. основные усилия были направлены на нахождение все более мощных достаточных условий. Наилучшие известные теперь достаточные условия, с одной стороны, являются очень мощными в том смысле, что *им удовлетворяют все простые числа, меньшие 100 000* [W1]. Однако, с другой стороны, все эти условия вызывают сильное разочарование, поскольку *среди них нет ни одного, которому удовлетворяло бы бесконечное множество*

*простых показателей.* Таким образом, Последнюю теорему Ферма можно доказать для любого простого числа, лежащего в доступных для вычислений пределах, и тем не менее нельзя исключить возможность, что для *всех* простых чисел, превосходящих некоторую большую границу, теорема *неверна*.

Основным методом изложения в этой книге, как указывает ее подзаголовок, является генетический метод. Словарь определяет «генетический» как «относящийся к генезису, происхождению». В этой книге я попытался объяснить основные методы и понятия алгебраической теории чисел и продемонстрировать их естественность и эффективность, прослеживая их происхождение и развитие в работах некоторых из великих мастеров: Ферма, Эйлера, Лагранжа, Лежандра, Гаусса, Дирихле, Куммера и других.

Важно отличать генетический метод от описания истории вопроса. Различие заключается в том, что генетический метод прежде всего занимается самим предметом изучения — его происхождением и развитием, тогда как основной целью исторического описания является аккуратная регистрация сведений о людях, идеях и событиях, которые играли роль в эволюции предмета изучения. В истории нет места для детального описания теории — если только это не является существенным для понимания событий. В генетическом методе нет места для внимательного изучения событий — если только это не способствует более глубокому проникновению в предмет.

Это означает, что генетический метод имеет тенденцию представлять историческую последовательность в искаженной перспективе. Игнорируются вопросы, которые так и не были успешно разрешены. Не рассматриваются идеи, ведущие в тупик. Генетический метод обходит молчанием месяцы бесплодных усилий и горы вспомогательных вычислений. Для того чтобы выявить действительно плодотворные идеи, приходится делать вид, что человеческий разум по прямой линии движется от задач к решениям. Я особенно хотел бы подчеркнуть, что представление о прямолинейном движении человеческого разума является настолько нелепой фикцией, что к ней ни на мгновение нельзя относиться серьезно.

Сэмюэль Джонсон некогда так писал о работе над биографиями: «Если бы дозволялось показывать лишь светлые стороны характеров, то нам оставалось бы только впасть в уныние из-за полной невозможности в чем-либо следовать героям. Авторы жизнеописаний святых рассказывали как о дурных, так и о добродетельных поступках людей. Это удерживало человечество от отчаяния, в чем и заключалось моральное действие такого подхода». В этой книге по большей части мы показываем только светлые стороны, только плодотворные идеи и только правильные догадки. Читатель должен иметь в виду, что эта книга *не является* ни исторической, ни биографической, и, значит, ему не стоит впадать в отчаяние.

Возможно, вас интересует не столько разница между историческим описанием и генетическим методом, сколько отличие генетического метода от более обычного метода математического изложения. Как утверждал математик Отто Теплиц, сущность генетического метода состоит в том, чтобы, рассмотрев исторические источники идеи, найти для нее наилучшую мотивировку, и, изучив контекст, в котором работал человек, первым выдвинувший эту идею, найти тот «жгучий вопрос», на который он жаждал ответить [Т1]. В противоположность этому более обычный метод оставляет в стороне вопросы и приводит лишь ответы. С логической точки зрения нужны только ответы, однако с психологической точки зрения изучать ответы, не зная вопросов, очень трудно и даже практически невозможно. По крайней мере таков мой собственный опыт. Я обнаружил, что наилучший путь преодолеть трудности изучения абстрактной математической теории состоит в том, чтобы последовать совету Теплица и игнорировать современные изложения до тех пор, пока не изучишь генезис и не узнаешь вопросов, которые привели к этой теории.

В первых трех главах этой книги рассматриваются элементарные аспекты Последней теоремы Ферма. Эти главы написаны на более элементарном уровне, чем остальная часть книги. Я надеюсь, что читателю, обладающему достаточной математической зрелостью для чтения последних глав, эти первые три главы тоже покажутся интересным и достойным внимания, хотя и легким чтением. В то же время я надеюсь, что менее искушенный читатель, который потратит больше времени и сил на первые главы, в результате приобретет достаточно опыта, чтобы, хотя и с трудом, но преодолеть и дальнейшие главы.

Следующие три главы 4—6 посвящены развитию куммеровской теории идеальных делителей и ее приложению к доказательству сформулированной выше замечательной теоремы Куммера о том, что Последняя теорема Ферма верна для регулярных простых показателей. Это наивысшая точка, которая достигается в настоящей книге при изучении Последней теоремы Ферма. Я намереваюсь написать второй том, в котором будут изложены работы по Последней теореме Ферма, выходящие за пределы теоремы Куммера; однако эти более поздние исследования трудны, и теорема Куммера является естественной точкой для завершения этого тома.

В трех последних главах рассматриваются вопросы, более косвенным образом связанные с Последней теоремой Ферма, а именно: теория идеального разложения для квадратичных целых, гауссова теория бинарных квадратичных форм и формула Дирихле для числа классов. Изучать работы Куммера по Последней теореме Ферма, не касаясь этих вопросов, столь же неразумно, как изучать историю Германии, не затрагивая истории Франции. С самого начала своей работы по теории идеалов Куммер созна-

вал, что она тесно связана с гауссовой теорией бинарных квадратичных форм. Применение к Последней теореме Ферма было лишь одним из мотивов, побудивших Куммера к развитию этой теории; другими мотивами (и, по его собственному свидетельству, более настоящими) были поиски обобщения квадратичного, кубического и биквадратичного законов взаимности на высшие степени и попытки найти объяснение трудной гауссовой теории композиции форм. Кроме того, по словам самого Куммера, тем, что ему удалось удивительно быстро найти формулу для числа классов и открыть поразительную связь между Последней теоремой Ферма для показателя  $p$  и поведением чисел Бернулли по модулю  $p$ , он был обязан решению Дирихле аналогичной задачи в квадратичном случае. Генетический метод подсказывает — почти требует — изучить эти достижения и найти мотивировку трудной, но чрезвычайно плодотворной идеи «идеальных простых делителей», столь существенной для понимания работ Куммера по Последней теореме Ферма. Кроме того, материал трех заключительных глав обеспечивает необходимую основу для изучения высших законов взаимности и теории полей классов, на которые в свою очередь опираются более поздние работы по Последней теореме Ферма, намеченные для изучения во втором томе.

В этой книге, как в основном тексте, так и в упражнениях, особенно большое место уделено *вычислениям*. Это необходимая составляющая генетического метода. Действительно, даже поверхностный взгляд на историю вопроса показывает, что Куммер и другие великие новаторы в теории чисел производили обширные вычисления и на этом пути достигали своих глубоких озарений. Я вынужден с прискорбием заметить, что современное математическое образование имеет тенденцию прививать студентам мысль, что вычисления являются унизительной нудной работой, которой следует избегать любой ценой. Если вы внимательно проследите за вычислениями в основном тексте и будете рассматривать упражнения вычислительного характера не только как отнимающие время (неизбежно они обладают этой особенностью), но и как представляющие интерес, доставляющие наслаждение и понимание, то я уверен, что вы сможете оценить как мощь, так и крайнюю простоту теории.

Я убежден в том, что не бывает пассивного понимания математики. Только при активном чтении лекций, написании учебников или решении задач можно полностью овладеть математическими идеями. Именно по этой причине данная книга содержит так много упражнений, и именно по этой причине я считал, что серьезный читатель должен решить их как можно больше. Некоторые из моих коллег указали мне, что, предлагая столь большое количество упражнений, я оттолкну от книги тех читателей, которые захотели бы прочитать ее только ради удовольствия. На это я могу



ответить, что упражнения только предлагаются, но не предписываются для обязательного решения. Делайте с ними что хотите, но, возможно, вы обнаружите, что они также способны доставить удовольствие.

Знаменитая премия за доказательство Последней теоремы Ферма была учреждена П. Вольфскем в 1908 г. Одним из условий присуждения премии была публикация доказательства, и, по-видимому, главным результатом учреждения премии было чудовищное количество нелепых доказательств, предназначенных для печати или опубликованных частным образом. С очевидным удовольствием Морделл и другие специалисты по теории чисел объявили, что последовавшая после первой мировой войны инфляция в Германии свела первоначально внушительную премию практически к нулю. Однако экономическое возрождение ФРГ после второй мировой войны изменило ситуацию. Теперь премия Вольфскеля составляет около 10 000 западногерманских марок, или 4000 американских долларов. Для присуждения премии доказательство должно быть опубликовано и не менее чем через два года после публикации должно быть признано верным Геттингенской Академией наук.

Если вы намерены попытаться заработать эту премию — примите мои наилучшие пожелания. Я был бы восхищен, если бы эта задача была решена, и особенно если бы человеку, решившему ее, оказалась полезной моя книга. И хотя можно спорить о том, способна ли книга, излагающая идеи, которые *не привели* к решению задачи, оказаться полезной тому, кто надеется найти решение, я думаю, что безуспешных усилий многих первоклассных математиков (не говоря уже о многих не таких первоклассных) достаточно для того, чтобы считать наивный подход к этой проблеме совершенно безнадежным. Приведенные в этой книге идеи *позволяют* решить проблему для всех показателей, меньших 37. Ничего подобного нельзя сказать ни об одном подходе, не использующем куммерову теорию идеального разложения. Однако прежде чем вы задумаете добиться получения премии Вольфскеля, стоит принять во внимание еще одно обстоятельство. Мне кажется, что нет вообще никаких оснований считать Последнюю теорему Ферма верной, а условия присуждения премии не предлагают ни единого пфеннига за опровержение этой теоремы.

### *Благодарности*

Просто сказать, что работа над книгой велась при финансовой поддержке фонда Вона, значило бы создать совершенно неправильное представление о том, до какой степени я обязан этому фонду и лично г-ну Джеймсу М. Вону, мл. Если бы я не получил

от них предложения рассказать о Последней теореме Ферма, эта книга не только никогда не появилась бы, но у меня и не возникла бы мысль писать ее. Я глубоко благодарен г-ну Вону и фонду за приглашение заняться этим столь увлекательным, полезным и приятным делом. Я хотел бы также поблагодарить Брюса Чендлера за дружескую поддержку и мудрые советы. Его семинар по истории математики в Нью-Йоркском университете стал замечательным местом встреч историков математики — встреч, которые я и многие другие считаем чрезвычайно полезными и вдохновляющими.

Кроме того, я признателен многим ученым, высказавшим свои замечания по рукописи. В частности, я хотел бы упомянуть Джона Бриллхарта, Эда Кертиса, Пьера Дюгака, Дж. М. Ганди, Линетт Ганим, Поля Халмоша, Жана Итара, Вальтера Кауфман-Бюлера, Морриса Клайна, Карлоса Морено, Эла Новикова, Гарольда Шапиро, Габриэля Штольценберга, Джеймса Вона и Андре Вейля.

Наконец, я благодарен Курантовскому институту математических наук при Нью-Йоркском университете за удобное рабочее место, отличную библиотеку и высококвалифицированную работу Элен Саморай и ее коллег по перепечатке рукописи.

*Гарольд М. Эдвардс*

## Глава 1

### ФЕРМА

#### 1.1. Ферма и его «Последняя теорема»

Пьер де Ферма умер в 1665 г. К этому времени он был одним из самых знаменитых математиков Европы. Сегодня имя Ферма неотделимо от теории чисел, но при жизни его работы по теории чисел были настолько революционными и настолько опережали свое время, что их значение было плохо понято современниками, и слава Ферма основывалась больше на его достижениях в других областях науки. Среди них были важные труды по аналитической геометрии (независимо от Декарта Ферма был одним из создателей этой науки), по теории касательных, вычисления площадей, максимумов и минимумов (эти работы послужили началом математического анализа) и по геометрической оптике (которую он обогатил открытием того, что законы преломления можно вывести из принципа наименьшего времени).

В славе Ферма как математика есть два удивительных факта. Во-первых, по профессии Ферма был юристом, а не математиком. В зрелом возрасте он занимал довольно важные судебные должности в Тулузе, посвящая математике лишь свободное время. Во-вторых, за всю свою жизнь он не опубликовал ни одной математической работы<sup>1)</sup>. Своей репутацией Ферма был обязан переписке с другими учеными и значительному количеству трактатов, которые распространялись в рукописном виде. Ферма часто убеждали опубликовать его работы, но по необъяснимым причинам он отказывался печатать свои труды, и многие из его открытий, особенно в теории чисел, так и не были приведены к виду, пригодному для публикации.

Поскольку Ферма отказывался публиковать свои работы, многие из его почитателей стали опасаться, что он скоро будет забыт, если не попытаться собрать его письма и неопубликованные трактаты и издать их посмертно. Такая попытка была предпринята его сыном, Самюэлем. Самюэль де Ферма занялся не только сбором

---

<sup>1)</sup> Есть одно небольшое исключение. В 1660 г. он разрешил опубликовать второстепенную работу в качестве приложения к книге, написанной его коллегой. Однако это исключение лишь подтверждает правило: работа была опубликована анонимно.

писем и трактатов среди корреспондентов отца, но и разобрал его бумаги и книги, и именно этот путь привел к публикации знаменитой «Последней теоремы» Ферма.

Книгой, первоначально вдохновившей Ферма на изучение теории чисел, была «Арифметика» Диофанта — одно из великих классических произведений древнегреческой математики, незадолго до того переоткрытое и переведенное на латинский язык. Самюэль обнаружил, что его отец сделал много замечаний на полях своего экземпляра книги Диофанта в переводе Баше, и для начала он выпустил новое издание «Арифметики» Диофанта [D3], которое в качестве приложения содержало сделанные Ферма заметки на полях. Второе из этих 48 «Замечаний к Диофанту» было написано на полях вслед за задачей 8 из Книги II. В этой задаче требуется «данное число, которое является квадратом, записать в виде суммы двух других квадратов».

Написанная на латинском языке заметка Ферма утверждает, что «с другой стороны, невозможно куб записать в виде суммы двух кубов, или четвертую степень — в виде суммы двух четвертых степеней, или, вообще, любое число, которое является степенью большей, чем вторая, нельзя записать в виде суммы двух таких же степеней. У меня есть поистине удивительное доказательство этого утверждения, но поля эти слишком узки, чтобы его уместить». Это простое утверждение, которое символически можно записать так: «для любого целого  $n > 2$  уравнение  $x^n + y^n = z^n$  неразрешимо», — теперь известно как *Последняя теорема Ферма*. Если Ферма действительно знал доказательство этого утверждения, оно несомненно было «удивительным», поскольку за триста с лишним лет, прошедших со времен Ферма, никто больше не смог найти такого доказательства. Эту задачу безуспешно пытались решить многие великие математики, и хотя был достигнут некоторый прогресс, позволивший доказать утверждение Ферма для всех показателей  $n$  порядка многих тысяч, до сегодняшнего дня неизвестно, справедливо это утверждение или нет.

Происхождение названия «Последняя теорема Ферма» неясно. Неизвестно, в какой период жизни Ферма написал эту заметку на полях, но принято считать, что он написал ее тогда, когда впервые изучал книгу Диофанта, т. е. в конце 1630-х годов, — за три десятилетия до смерти. В таком случае эта теорема, конечно, не была его последней теоремой. Вполне возможно, что это название обязано своим происхождением тому обстоятельству, что среди многих теорем, которые Ферма сформулировал без доказательства, эта теорема остается последней, до сих пор не доказанной. По-видимому, заслуживает внимания и соображение о том, что Ферма после дальнейших размышлений был, возможно, не вполне удовлетворен своим «удивительным доказательством», особенно если он действительно написал о нем в 1630-е годы. В самом деле,

другие теоремы он вновь и вновь формулирует в своих письмах (иногда в виде своеобразного вызова на соревнование); среди них встречаются и частные случаи  $x^3 + y^3 \neq z^3$ ,  $x^4 + y^4 \neq z^4$ . Последней теоремы, но сама эта теорема появилась лишь однажды как замечание номер 2 к Диофанту — загадочным сфинксом для потомков.

В «Арифметике» Диофанта рассматриваются исключительно рациональные числа, поэтому не следует сомневаться в том, что Ферма имел в виду отсутствие *рациональных* чисел  $x, y, z$ , таких, что  $x^n + y^n = z^n$  ( $n > 2$ ). Если бы можно было рассматривать иррациональные числа, то для любой пары чисел  $x, y$  мы получили бы такое решение, просто положив  $z = \sqrt[n]{x^n + y^n}$ . С другой стороны, если бы уравнение  $x^n + y^n = z^n$  имело рациональные решения, то оно имело бы и *целые* решения, или *решения в целых числах*: действительно, если  $x, y, z$  — рациональные решения уравнения  $x^n + y^n = z^n$  и  $d$  — их наименьший общий знаменатель, то  $xd, yd, zd$  — целые числа и  $(xd)^n + (yd)^n = (x^n + y^n) d^n = (zd)^n$ , так что  $zd$  — целое число,  $n$ -я степень которого равна сумме  $n$ -х степеней. Кроме того, как Диофант, так и Ферма имели дело с *положительными* числами — во времена Ферма к отрицательным числам и нулю еще относились с подозрением, — поэтому молчаливо исключается также и тривиальный случай, когда  $x$  или  $y$  равно нулю. (Например, равенство  $2^5 + 0^5 = 2^5$ , конечно, не противоречит Последней теореме Ферма.) Таким образом, Последняя теорема Ферма, по существу, сводится к утверждению о том, что если  $n$  — целое, большее двух, то невозможно найти такие положительные целые числа  $x, y, z$ , что  $x^n + y^n = z^n$ . Именно в таком виде обычно и формулируется эта теорема.

За три столетия, прошедшие после смерти Ферма, его работы во всех областях, кроме теории чисел, были постепенно забыты, но не потому, что они оказались чем-либо плохи. Наоборот, это были первые серьезные шаги в развитии важных теорий, которые теперь значительно яснее поняты и которые проще объяснить с использованием языка и символики, не существовавших во времена Ферма. В то же время работы Ферма по теории чисел пользуются непреходящей славой, и среди них не только его Последняя теорема, но и многие другие открытия и идеи, часть которых мы рассмотрим позже в этой главе. Такое отношение к наследию Ферма кажется вполне сообразным, поскольку, как явствует из его переписки, какими бы важными для развития математики ни считал он свои работы в других областях, его истинной любовью была теория чисел, изучение свойств положительных целых чисел, которые казались ему величайшим вызовом силе чистого математического рассуждения и величайшей сокровищницей чистых математических истин.

## 1.2. Пифагоровы треугольники

В предложении из «Арифметики» Диофанта, которое привело Ферма к его Последней теореме, рассматривается одна из самых старых математических задач: «записать квадрат в виде суммы двух квадратов». Одно решение этой задачи получается при помощи равенства  $3^2 + 4^2 = 5^2$ , из которого следует, что для любого квадрата  $a^2$  справедливо тождество  $a^2 = (3a/5)^2 + (4a/5)^2$ . Аналогично, любая тройка положительных целых  $x, y, z$ , таких, что  $x^2 + y^2 = z^2$ , дает решение  $a^2 = (xa/z)^2 + (ya/z)^2$ , и, как легко видеть, любое решение получается таким образом. Короче говоря, задача Диофанта сводится к задаче нахождения троек положительных целых чисел, удовлетворяющих уравнению  $x^2 + y^2 = z^2$ .

Если задачу Диофанта сформулировать таким образом, то станет очевидной ее связь с теоремой Пифагора. По теореме Пифагора <sup>1)</sup> из равенства  $3^2 + 4^2 = 5^2$  следует, что треугольник, стороны которого находятся в отношении  $3 : 4 : 5$ , является прямоугольным треугольником. Вообще, любая тройка положительных целых  $x, y, z$ , удовлетворяющая уравнению  $x^2 + y^2 = z^2$ , определяет такое множество отношений  $x : y : z$ , что треугольник, стороны которого находятся в этом отношении, является прямоугольным треугольником. Это означает, что задачу Диофанта можно на геометрическом языке выразить как задачу нахождения прямоугольных треугольников с *соизмеримыми* <sup>2)</sup> длинами сторон, т. е. треугольников, для которых отношения длин сторон выражаются как отношения целых чисел. Ввиду такой геометрической интерпретации любую тройку положительных целых чисел, удовлетворяющую уравнению  $x^2 + y^2 = z^2$ , называют *пифагоровой тройкой*.

Пифагорова тройка  $3^2 + 4^2 = 5^2$  — самый простой и наиболее известный пример. Другой пример:  $5^2 + 12^2 = 13^2$ . Конечно, здесь важны только отношения, и тройка 6, 8, 10, которая образует те же отношения, что и 3, 4, 5, также является пифагоровой тройкой. Аналогично, 9, 12, 15 и 10, 24, 26 — пифагоровы трой-

---

<sup>1)</sup> Если теорема Пифагора сформулирована в своем обычном виде как утверждение о том, что «в прямоугольном треугольнике квадрат, построенный на гипотенузе, равен сумме квадратов, построенных на катетах», то здесь требуется теорема, обратная к теореме Пифагора. Однако из более сильной формы теоремы: «если  $a, b, c$  — стороны треугольника, то угол, противолежащий стороне  $c$ , является острым, прямым или тупым в зависимости от того больше, равно или меньше  $a^2 + b^2$  чем  $c^2$ », следует обратное утверждение: «если  $a^2 + b^2 = c^2$ , то данный треугольник является прямоугольным».

<sup>2)</sup> Концепция соизмеримости является центральной в греческой математике; рассмотрению этого понятия посвящена значительная часть «Начал» Евклида. Одной из основных вдохновляющих идей греческой математики было открытие Пифагора, согласно которому стороны равнобедренного прямоугольного треугольника несоизмеримы, или, что то же самое, число  $\sqrt{2}$  иррационально.



ки, которые существенно не отличаются от приведенных выше. Но тройка 7, 24, 25 отличается существенно. Задача Диофанта состоит в нахождении пифагоровых троек. За несколько веков до Диофанта (около 250 г. н. э.?) эту задачу рассмотрел Евклид (около 300 г. до н. э.) в своих «Началах» (Книга X, лемма 1 между предложениями 28 и 29). Однако, как показало одно из самых удивительных открытий археологии двадцатого века, более чем за тысячу лет до Евклида эту задачу изучали древние вавилоняне.

В археологической коллекции Колумбийского университета хранится клинописная табличка, датируемая приблизительно 1500 г. до н. э.; при изучении оказалось (см. Нейгебауэр [N1]), что она содержит список пифагоровых троек. Одна из троек в этом списке — 3, 4, 5, но среди других содержится также и 4961, 6480, 8161. (Возможно, читателю будет интересно провести вычисления и убедиться в том, что это действительно пифагорова тройка.) Эта тройка со всей достоверностью показывает, что список был составлен каким-то методом, отличным от метода проб и ошибок; значит, древние вавилоняне обладали каким-то способом решения задачи Диофанта. Мы не знаем ни того, что это был за способ, ни того, какие причины побудили вавилонян изучать пифагоровы тройки. По мнению Нейгебауэра, вполне вероятно, что им был известен геометрический смысл пифагоровых троек — другими словами, вавилоняне знали теорему Пифагора за тысячу лет до Пифагора, — и что они получали эти тройки каким-то методом, подобным использованному в книгах Диофанта и, с меньшей строгостью, Евклида. Этот метод мы рассмотрим в следующем параграфе.

Интересно, и, по-видимому, это не простое совпадение, что этой задаче из предыстории математики суждено было привести к одной из самых знаменитых математических задач нашего времени.

### 1.3. Как находить пифагоровы тройки

Хотя идеи следующего решения задачи нахождения пифагоровых троек, по существу, совпадают с идеями решения Диофанта <sup>1)</sup>, наши обозначения, терминология и изложение современны. Конечно, серьезному студенту стоит прочесть собственное изложение Диофанта (имеется прекрасный английский перевод Хита [H1]), но для того, чтобы восстановить обозначения и точку зрения Диофанта, требуются некоторые усилия, и, поскольку в нашей книге рассматривается более современная математика, мы не будем

---

<sup>1)</sup> Довольно странно, что это решение появляется у Диофанта не как решение задачи «записать квадрат в виде суммы двух квадратов» из Книги II, а как одно из решений задач, связанных с прямоугольными треугольниками. См. стр. 93 издания Хита книги Диофанта [H1].

предпринимать попытку такой реконструкции. Рассуждение в этом доказательстве является очень важным, и его основная идея снова и снова встречается при изучении Последней теоремы Ферма.

Метод приводимого ниже решения известен в классической греческой математике как *аналитический* метод<sup>1)</sup>: предполагается, что задано некоторое решение уравнения  $x^2 + y^2 = z^2$  ( $x, y, z$  — положительные целые), и свойства данного решения *анализируются* с тем, чтобы найти такие характеристики этих решений, которые позволили бы их строить.

Заметим прежде всего, что если  $d$  — некоторое число, на которое делятся все три числа  $x, y, z$ , то уравнение  $x^2 + y^2 = z^2$  можно сократить на  $d^2$  и целые  $x/d, y/d, z/d$  также составляют пифагорову тройку. Если  $d$  — наибольший общий делитель чисел  $x, y, z$ , то  $x/d, y/d, z/d$  не имеют общих делителей, отличных от 1, и образуют так называемую *примитивную* пифагорову тройку, т. е. пифагорову тройку, входящие в которую числа не имеют общих делителей, отличных от 1. Таким способом — делением на наибольший общий делитель — каждую пифагорову тройку можно привести к примитивной. Обратно, если дана примитивная пифагорова тройка, скажем  $a^2 + b^2 = c^2$ , то любая пифагорова тройка, которая приводится к ней, может быть получена путем выбора соответствующего целого  $d$  и умножения на него:  $x = ad, y = bd, z = cd$ . Следовательно, достаточно научиться находить примитивные пифагоровы тройки и с самого начала можно предположить, что данная тройка  $x, y, z$  примитивная.

Из этого предположения следует, что никакие два из трех чисел  $x, y, z$  не имеют общих делителей, больших 1. Например, если бы  $d$  было делителем  $x$  и  $y$ , то из равенства  $z^2 = x^2 + y^2$  следовало бы, что  $d^2$  является делителем  $z^2$ , а тем самым<sup>2)</sup>, что  $d$  делит  $z$ . Следовательно,  $d$  делило бы все три числа и, согласно примитивности тройки, равнялось бы 1. Аналогично, единственным общим делителем  $x$  и  $z$  или  $y$  и  $z$  служит 1.

В частности, никакие два из трех чисел  $x, y, z$  не могут быть четными (иметь общий делитель 2). Следовательно, по крайней мере два из них нечетны. Но очевидно, что все три числа не могут быть нечетными, так как тогда из  $x^2 + y^2 = z^2$  следовало бы, что «нечетное + нечетное = нечетное», а это невозможно. Поэтому в точности одно из них четно. Рассматривая сравнения по модулю 4, легко видеть, что  $z$  не может быть четным. Действительно, квадрат нечетного числа  $2n + 1$  на единицу больше некоторого

<sup>1)</sup> См. «Собрание» Паппа.

<sup>2)</sup> Доказательство этого факта см. в упр. 3. Кратко его идея такова: квадрат несократимой дроби сам является несократимой дробью, следовательно,  $(z/d)^2$  может быть целым числом только тогда, когда  $z/d$  — целое.



числа, кратного 4, а именно, он равен  $4n^2 + 4n + 1$ . Квадрат четного числа кратен 4: он равен  $4n^2$ . Таким образом, если бы  $x$  и  $y$  были нечетными, а  $z$  четным, то равенство  $x^2 + y^2 = z^2$  давало бы нам число, кратное 4 и одновременно равное сумме двух чисел, каждое из которых на единицу больше, чем некоторое число, кратное 4, что, очевидно, невозможно. Следовательно,  $z$  нечетно, а  $x$  и  $y$  имеют противоположную четность: одно из них нечетно, а другое — четно. В случае необходимости меняя местами  $x$  и  $y$ , мы можем считать, что в данной примитивной пифагоровой тройке  $x$  четно, тогда как  $y$  и  $z$  нечетны.

Теперь перепишем уравнение  $x^2 + y^2 = z^2$  в виде  $x^2 = z^2 - y^2$  и, разложив правую часть на множители, получим  $x^2 = (z + y)(z - y)$ . Поскольку все числа  $x$ ,  $z + y$  и  $z - y$  четны, существуют такие положительные целые  $u$ ,  $v$ ,  $w$ , что  $x = 2u$ ,  $z + y = 2v$ ,  $z - y = 2w$ . Тогда  $(2u)^2 = (2v)(2w)$ , или  $u^2 = vw$ . Кроме того, наибольший общий делитель  $v$  и  $w$  равен 1, так как любое число, делящее как  $v$ , так и  $w$ , делило бы также и  $v + w = \frac{1}{2}(z + y) + \frac{1}{2}(z - y) = \frac{1}{2}(2z) = z$  и  $v - w = \frac{1}{2}(z + y) - \frac{1}{2}(z - y) = y$  и потому могло бы равняться только 1. Другими словами,  $v$  и  $w$  взаимно просты.

Основной шаг нашего рассуждения состоит в следующем. *Произведение двух взаимно простых чисел  $v$  и  $w$  может быть квадратом  $vw = u^2$  только тогда, когда  $v$  и  $w$  сами являются квадратами.* Это утверждение становится очевидным, если мы рассмотрим разложение чисел  $v$  и  $w$  на простые множители. Действительно, поскольку  $v$  и  $w$  взаимно просты, то ни одно простое не входит одновременно в разложения  $v$  и  $w$ . Поэтому разложение числа  $vw$  на простые множители распадается на эти два разложения; если  $vw$  является квадратом, то все простые должны входить в разложение  $vw$  в четных степенях, но тогда они должны входить уже в разложения  $v$  и  $w$  в четных степенях. Следовательно,  $v$  и  $w$  — квадраты. Полное доказательство этого утверждения будет приведено в следующем параграфе.

Итак, существуют такие положительные целые  $p$  и  $q$ , что  $v = p^2$ ,  $w = q^2$ . Кроме того,  $p$  и  $q$  взаимно просты, поскольку таковы  $v$  и  $w$ . Тогда

$$\begin{aligned} z &= v + w = p^2 + q^2, \\ y &= v - w = p^2 - q^2. \end{aligned}$$

Это показывает, что  $p$  больше  $q$  ( $y$  положительно) и что  $p$  и  $q$  должны иметь противоположную четность (поскольку  $z$  и  $y$  нечетны). Далее,  $x$  легко выразить через  $p$  и  $q$ :

$$\begin{aligned} x^2 &= z^2 - y^2 = p^4 + 2p^2q^2 + q^4 - p^4 + 2p^2q^2 - q^4 = 4p^2q^2 = (2pq)^2, \\ x &= 2pq. \end{aligned}$$

Таким образом, если дана произвольная примитивная пифагорова тройка, то найдутся такие взаимно простые положительные целые  $p$  и  $q$ , что  $p > q$ ,  $p$  и  $q$  имеют противоположную четность и данная тройка состоит из чисел  $2pq$ ,  $p^2 - q^2$  и  $p^2 + q^2$ .

Это завершает анализ, поскольку легко доказать, что если дана произвольная пара  $p$  и  $q$ , такая, что (1)  $p$  и  $q$  взаимно просты, (2)  $p > q$  и (3)  $p$  и  $q$  имеют противоположную четность, то числа  $2pq$ ,  $p^2 - q^2$ ,  $p^2 + q^2$  образуют примитивную пифагорову тройку. Для этого достаточно заметить, что

$$(2pq)^2 + (p^2 - q^2)^2 = (p^2 + q^2)^2$$

является алгебраическим тождеством, справедливым для всех  $p$  и  $q$ , и что из условий, наложенных на  $p$  и  $q$ , следует, что  $2pq$  и  $p^2 - q^2$  взаимно просты (и, значит, соответствующая тройка примитивна). Действительно, если бы эти числа имели общий делитель, больший 1, то они имели бы и простой общий делитель, скажем  $P$ . Поскольку  $p^2 - q^2$  нечетно,  $P$  не равно 2; поэтому на  $P$  должно делиться  $p$  или  $q$  (так как на него делится  $2pq$ ), но не оба эти числа одновременно (так как  $p$  и  $q$  взаимно просты). Но это невозможно, поскольку это противоречило бы предположению о том, что  $P$  делит  $p^2 - q^2$ .

Это полностью решает задачу построения пифагоровых троек. Все пифагоровы тройки, соответствующие парам  $p$  и  $q$  с  $p \leq 8$ , приведены в табл. 1.1. Заметим, что в эту таблицу входят стандарт-

Таблица 1.1. Пифагоровы тройки

$p$	$q$	$x$	$y$	$z$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85
8	1	16	63	65
8	3	48	55	73
8	5	80	39	89
8	7	112	15	113

ные примеры 3, 4, 5; 5, 12, 13 и 7, 24, 25. Заметим также, что легко продолжить эту таблицу на бóльшие значения  $p$ , включая только те значения  $q$ , которые меньше  $p$ , взаимно просты с  $p$  и имеют противоположную четность.

## Упражнения

1. Найдите значения  $p$  и  $q$ , которые соответствуют пифагоровой тройке из вавилонской таблички, приведенной в § 1.2.

2. Продолжите таблицу 1.1 до  $p = 12$ .

3. В следующем параграфе будет доказано, что если  $vw = u^2$  и  $v, w$  взаимно просты, то  $v$  и  $w$  являются квадратами. Используйте это для доказательства того, что если  $d^2$  делит  $z^2$ , то  $d$  делит  $z$ . [Пусть  $d = cD$ ,  $z = cZ$ , где  $c$  — наибольший общий делитель  $d$  и  $z$ . Тогда  $Z^2 = kD^2$ , где  $k$  и  $D^2$  взаимно просты.]

## 1.4. Метод бесконечного спуска

Метод бесконечного спуска изобрел Ферма, и этим изобретением он чрезвычайно гордился. В длинном письме, написанном незадолго до смерти, он подвел итог своим открытиям в теории чисел и с полной определенностью заявил, что во всех своих доказательствах пользовался этим методом. Коротко говоря, этот метод состоит в следующем: некоторые свойства или отношения невозможны для целых чисел, если исходя из предположения о том, что они выполняются для каких-либо чисел, удастся доказать, что они выполняются для некоторых меньших чисел. Действительно, в таком случае то же самое рассуждение позволяет заключить, что они выполняются для еще меньших чисел, и т. д. — *ad infinitum*, — что невозможно, поскольку последовательность положительных целых чисел не может бесконечно убывать.

Например, рассмотрим предложение, которое мы использовали в предыдущем параграфе, а именно: *если  $v$  и  $w$  взаимно просты и  $vw$  является квадратом, то и сами  $v$  и  $w$  должны быть квадратами*. Как подчеркивал сам Ферма, метод бесконечного спуска — это метод доказательства *невозможности*. В рассматриваемом случае мы должны доказать, что невозможно найти такие числа  $v$  и  $w$ , что (1)  $v$  и  $w$  взаимно просты, (2)  $vw$  — квадрат и (3)  $v$  или  $w$  не является квадратом.

Предположим, что можно найти такие  $v$  и  $w$ . В случае необходимости меняя местами  $v$  и  $w$ , мы можем предположить, что  $v$  не является квадратом. В частности,  $v \neq 1$ . Следовательно,  $v$  делится по крайней мере на одно простое число. Пусть  $P$  — какое-либо простое число, на которое делится  $v$ , скажем  $v = Pk$ . Тогда на  $P$  делится также число  $vw$ , которое является квадратом:  $vw = u^2$ . Согласно основному свойству простых чисел (см. приложение, § A.1), если  $P$  делит  $u \cdot u$ , то  $P$  должно делить  $u$  или  $u$ , т. е.  $P$

должно делить  $u$ :  $u = Pt$ . Тогда равенство  $vw = u^2$  можно переписать в виде  $Pkw = (Pt)^2 = P^2t^2$ ; отсюда следует, что  $kw = Pt^2$ . Так как  $P$  делит правую часть этого равенства, оно должно делить и левую. Следовательно, согласно основному свойству простых чисел,  $P$  должно делить либо  $k$ , либо  $w$ . Но  $P$  не делит  $w$ , поскольку оно делит  $v$ , а  $v$  и  $w$  взаимно просты. Поэтому  $P$  делит  $k$ , скажем  $k = Pv'$ . Тогда равенство  $kw = Pt^2$  превращается в  $Pv'w = Pt^2$ ; таким образом,  $v'w = t^2$ . Так как  $v = Pk = P^2v'$ , то любой делитель числа  $v'$  является делителем  $v$ , а следовательно,  $v'$  и  $w$  не могут иметь общих делителей, больших 1. Кроме того, если бы  $v'$  было квадратом, то число  $v = P^2v'$  также было бы квадратом, что не имеет места; поэтому  $v'$  не является квадратом. Таким образом, числа  $v', w$  обладают приведенными выше свойствами (1), (2), (3) и  $v' < v$ . Тогда то же самое рассуждение показывает, что существует другое положительное целое  $v'' < v'$ , такое, что  $v'', w$  обладают всеми этими тремя свойствами. Бесконечное повторение этих рассуждений привело бы нас к бесконечно убывающей последовательности положительных целых чисел  $v > v' > v'' > v''' > \dots$ . Но такой последовательности не существует (само число  $v$  дает верхнюю границу числа шагов, в течение которых оно может быть уменьшено), поэтому никакие два числа  $v$  и  $w$  не могут обладать тремя указанными свойствами. Это доказывает данное предложение.

Подводя итоги, можно сказать, что метод бесконечного спуска основывается на следующем принципе. *Если из предположения, согласно которому данное положительное целое обладает данным множеством свойств, следует, что существует меньшее положительное целое с тем же множеством свойств, то ни одно положительное целое не может обладать этим множеством свойств.*

### 1.5. Случай $n = 4$ Последней теоремы

Для доказательства Последней теоремы Ферма при  $n = 4$  достаточно, руководствуясь интуицией, сочетать методы двух предыдущих параграфов: метод бесконечного спуска и метод построения пифагоровых троек.

Предположим, что дано решение  $x, y, z$  уравнения  $x^4 + y^4 = z^4$ . Как и в случае пифагоровых троек, можно с самого начала считать, что  $x, y, z$  не имеют общих делителей, больших 1, и даже что никакие два из них не имеют общих делителей, больших 1. Действительно, в противном случае из равенства  $x^4 + y^4 = z^4$  следовало бы, что и третье из чисел имеет тот же самый делитель и уравнение можно сократить на четвертую степень этого делителя. Следовательно, числа  $x^2, y^2, z^2$  образуют примитивную пифагорову тройку и, в случае необходимости меняя местами  $x$  и  $y$ , можно

написать

$$x^2 = 2pq, \quad y^2 = p^2 - q^2, \quad z^2 = p^2 + q^2,$$

где  $p$  и  $q$  — взаимно простые числа противоположной четности и  $p > q > 0$ . Второе из этих уравнений можно записать в виде  $y^2 + q^2 = p^2$  и, поскольку  $p$  и  $q$  взаимно просты,  $y, q, p$  — примитивная пифагорова тройка. Таким образом,  $p$  нечетно, и так как  $p$  и  $q$  имеют противоположную четность, то  $q$  четно. Следовательно,

$$q = 2ab, \quad y = a^2 - b^2, \quad p = a^2 + b^2,$$

где  $a, b$  — взаимно простые числа противоположной четности и  $a > b > 0$ . Таким образом,

$$x^2 = 2pq = 4ab(a^2 + b^2).$$

Это показывает, что  $ab(a^2 + b^2)$  является квадратом, а именно квадратом половины четного числа  $x$ . Но  $ab$  и  $a^2 + b^2$  взаимно просты, поскольку любое простое  $P$ , делящее  $ab$ , делит  $a$  или  $b$  (по основному свойству простых чисел), но не оба этих числа одновременно (так как  $a$  и  $b$  взаимно просты), и поэтому не может делить  $a^2 + b^2$ . Следовательно, как  $ab$ , так и  $a^2 + b^2$  должны быть квадратами. Однако  $ab$  является квадратом, а целые  $a$  и  $b$  взаимно просты, поэтому как  $a$ , так и  $b$  должны быть квадратами, скажем  $a = X^2$ ,  $b = Y^2$ . Следовательно,  $X^4 + Y^4 = a^2 + b^2$  является квадратом. Теперь для того, чтобы привести в движение бесконечный спуск, достаточно заметить, что из исходного предположения  $x^4 + y^4 = z^4$  мы использовали лишь то, что  $z^4$  является *квадратом*, а не четвертой степенью. Другими словами, если  $x$  и  $y$  — такие положительные целые, что  $x^4 + y^4$  — квадрат, то приведенная выше последовательность шагов дает новую пару положительных целых  $X, Y$ , такую, что  $X^4 + Y^4$  является квадратом. Кроме того,  $X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4$ . Тем самым мы указали бесконечную убывающую последовательность положительных целых чисел, существование которой невозможно. Следовательно, сумма двух четвертых степеней не может быть даже квадратом, не говоря уже о четвертой степени. Это доказывает Последнюю теорему Ферма для четвертых степеней.

Отсюда, очевидно, следует, что при произвольном положительном целом  $m$  уравнение  $x^{4m} + y^{4m} = z^{4m}$  неразрешимо. Действительно, в противном случае тройка  $X = x^m, Y = y^m, Z = z^m$  была бы решением уравнения  $X^4 + Y^4 = Z^4$ . Таким образом, Последняя теорема Ферма справедлива для всех показателей  $n$ , которые делятся на 4. Показатель  $n > 2$ , который не делится на 4, не является степенью двойки и, следовательно, должен делиться на некоторое простое число  $p \neq 2$ ; например,  $n = pm$ . По той же

причине, что и выше, для доказательства неразрешимости уравнения  $x^n + y^n = z^n$ , очевидно, достаточно доказать, что неразрешимо уравнение  $x^p + y^p = z^p$ . Таким образом, *поскольку Последняя теорема Ферма доказана в случае  $n = 4$ , доказательство общего случая сводится к доказательству для простых  $n > 2$* . По этой причине в оставшейся части книги будут рассматриваться только те случаи Последней теоремы Ферма, в которых  $n$  — простое число,  $n \neq 2$ .

## 1.6. Одно доказательство Ферма

По-видимому, во всех дошедших до нас работах Ферма по теории чисел можно найти только одно доказательство. Это доказательство частного утверждения, которое Ферма неоднократно <sup>1)</sup> формулировал в своей переписке, но которое, как это характерно для Ферма, он не доказывал, оставляя эту задачу своим корреспондентам. Это доказательство, как и формулировка Последней теоремы, было обнаружено его сыном Самюэлем на полях все той же книги Диофанта; оно было включено в посмертно опубликованные работы как Замечание 45 к Диофанту.

В своих письмах Ферма часто повторяет, что у него нет желания скрывать свои работы, что, по его мнению, прогресс науки зависит от совместных усилий многих ученых и что он был бы счастлив открыть свои методы любому, кто пожелает. Однако факты красноречивее слов. То, что ни одно из многочисленных дошедших до нас писем Ферма не дает сколько-нибудь верного представления об используемых им методах, конечно, свидетельствует о том, что, сознательно или бессознательно, Ферма, как и все его современники, ревниво оберегал от соперников секреты своего ремесла.

В предложении, которое доказывает Ферма, утверждается, что *площадь прямоугольного треугольника не может быть квадратом*; здесь, конечно, имеется в виду, что площадь рационального прямоугольного треугольника не может равняться *рациональному* квадрату. Используя арифметическую операцию умножения всех длин на их наименьший общий знаменатель, или, что то же самое, геометрическую операцию выбора новой единицы длины, в которой стороны треугольника и квадрата задаются целыми числами (возвращаясь к греческой идее соизмеримости), можно переформулировать это предложение так: *не существует такой пифагоровой тройки  $x^2 + y^2 = z^2$ , что  $\frac{1}{2}xy$  является квадратом*. (Заметим, что  $x$  и  $y$  одновременно не могут быть нечетными, и поэтому  $\frac{1}{2}xy$

<sup>1)</sup> См. Диксон [D2], т. 2, стр. 616.



обязательно будет целым числом.) Именно в этом виде Ферма доказывает данное предложение.

Как характерно для задач, которыми занимался Ферма, эта задача не возникает из ничего, а основывается на предшествующей литературе. В Книге VI «Арифметики» Диофанта есть несколько задач, где требуется найти пифагоровы треугольники, площади которых удовлетворяют различным условиям, например отличаются от квадратов на данное положительное или отрицательное число. Однако Диофант, как всегда, удовлетворяется тем, что дает решение частных случаев своих задач, но не изучает условия, при которых данная задача имеет или не имеет решения. Ферма пользовался изданием книги Диофанта в переводе Баше (1581—1638), который не только перевел Диофанта с греческого на латынь, но и добавил к основному тексту многочисленные комментарии и дополнения. В своем дополнении к Книге VI Баше приводит необходимое и достаточное условие для того, чтобы число  $A$  было площадью пифагорова треугольника. Это условие состоит в существовании такого числа  $K$ , что  $(2A)^2 + K^4$  является квадратом<sup>1)</sup>. Таким образом, когда Ферма спрашивал, может ли треугольник иметь площадь, равную квадрату, он продолжал линию исследований, явно начатую Баше, который в свою очередь был вдохновлен на это Диофантом.

Приведенное Ферма доказательство этого предложения основано на более тонких соображениях, чем доказательство Последней теоремы для  $n = 4$  из предыдущего параграфа. Оно звучит следующим образом.

«Если бы площадь прямоугольного треугольника была квадратом, то существовали бы два биквадрата, разность которых была бы квадратом. Следовательно, существовали бы два квадрата, сумма и разность которых были бы квадратами. Поэтому мы получили бы квадрат, равный сумме некоторого квадрата и удвоенного другого квадрата, тогда как квадраты, из которых составлена эта сумма, сами давали бы в сумме квадрат. Но если квадрат составлен из квадрата и удвоенного другого квадрата, то его сторона, как я могу очень легко доказать, также составлена из квадрата и удвоенного другого квадрата. Отсюда мы заключаем, что указанная сторона является суммой сторон, прилежащих к прямому углу в прямоугольном треугольнике, и что простой квадрат, содержащийся в этой сумме, является основанием, а удвоенный квадрат — перпендикуляром.

Таким образом, этот прямоугольный треугольник образован из двух квадратов, сумма и разность которых также квадраты. Но можно доказать, что оба эти квадрата меньше, чем те квадраты, о которых мы первоначально предположили, что их сумма и разность являются квадратами. Следовательно, если существуют два таких квадрата, что их сумма и разность являются квадратами, то существуют также и два других целых квадрата с тем же свойством, но с меньшей суммой. Используя то же самое рассуждение, мы находим еще меньшую сумму, и так можно продолжать до бесконечности, находя все меньшие и меньшие квадраты целых чисел, обладающие тем же свойством. Это, однако, невозможно, поскольку не существует бесконечной последова-

<sup>1)</sup> См. Диксон [D2], т. 2, начало гл. XXII.

тельности чисел, меньших любого данного целого. Поля эти слишком узки для того, чтобы я мог дать доказательство полностью и со всеми деталями.» (Перевод на английский с латинского оригинала см. у Хита [Н1], стр. 293.)

Это доказательство, как вы обнаружите, если проследите его шаг за шагом, совершенно неясно в двух важных моментах.

В первом предложении разобраться достаточно легко. Самая общая пифагорова тройка имеет вид  $x = (2pq) d$ ,  $y = (p^2 - q^2) d$ ,  $z = (p^2 + q^2) d$  ( $p$  и  $q$  — взаимно простые положительные целые числа противоположной четности с  $p > q$ ,  $d$  — положительное целое), и задача состоит в том, чтобы представить  $\frac{1}{2} xy = pq(p^2 - q^2) d^2$  в виде квадрата. Это возможно тогда и только тогда, когда  $pq(p^2 - q^2)$  является квадратом. (Если  $Ad^2$  является квадратом, то  $A$  должно быть квадратом; см. упр. 1.) Поскольку  $p$  и  $q$  взаимно просты, каждое из них должно быть взаимно просто с  $p^2 - q^2$ . Следовательно,  $pq(p^2 - q^2)$  может быть квадратом только тогда, когда все числа  $p$ ,  $q$  и  $p^2 - q^2$  являются квадратами. Другими словами, треугольник, площадь которого является квадратом, приводит к паре таких взаимно простых чисел  $p$  и  $q$  противоположной четности, что  $p$ ,  $q$  и  $p^2 - q^2$  являются квадратами. Поскольку  $p$  и  $q$  — квадраты,  $p^2 - q^2$  является разностью четвертых степеней (биквадратов); это те самые «два биквадрата» Ферма, «разность которых равна квадрату». Кроме того,  $p^2 - q^2 = (p - q)(p + q)$  — разложение числа  $p^2 - q^2$  на два взаимно простых множителя. Действительно, любой общий делитель чисел  $p - q$  и  $p + q$  должен также делить  $(p - q) + (p + q) = 2p$  и  $(p + q) - (p - q) = 2q$ . Поскольку  $p$  и  $q$  взаимно просты, этот общий делитель может быть равен только числам 2 или 1. Однако  $p$  и  $q$  имеют противоположную четность, следовательно,  $p - q$  и  $p + q$  нечетны и у них нет общего делителя, отличного от 1. Поэтому из предположения о том, что  $p^2 - q^2$  является квадратом, следует, что  $p - q$  и  $p + q$  также являются квадратами. Это «два квадрата» Ферма, «сумма и разность которых являются квадратами». Третье предложение Ферма относится к равенствам  $(p - q) + 2q = p + q$ ,  $(p - q) + q = p$ , в которых числа  $p$ ,  $q$ ,  $p - q$  и  $p + q$  — квадраты.

В следующих двух предложениях разобраться уже трудно. Пусть  $p + q = r^2$ ,  $p - q = s^2$ . В первом из этих двух предложений утверждается, что  $r$  можно представить в виде  $r = u + v$ , где одно из чисел  $u$ ,  $v$  является квадратом, а второе — удвоенным квадратом. Во втором предложении говорится, что  $u$  и  $v$  являются сторонами прямоугольного треугольника, т. е. что  $u^2 + v^2$  — квадрат. О доказательстве первого утверждения <sup>1)</sup> Ферма говорит

<sup>1)</sup> Приведенное Ферма утверждение неточно, поскольку  $15^2 = 5^2 + 2 \cdot 10^2$ , но 15 не равно квадрату плюс удвоенный квадрат. Однако в рассматриваемом случае его заключение справедливо, так как  $r^2 = (p - q) + 2q$ , где  $p - q$  и  $q$  — взаимно простые квадраты.



лишь то, что он может «легко» его доказать; но даже если это и так, то не видно никакого пути для того, чтобы из первого утверждения «вывести» справедливость второго. Поэтому интерпретация этих предложений может быть лишь предположительной. Следующая интерпретация (по существу, принадлежащая Диксону [D2], т. 2, стр. 615—616) может совпадать или не совпадать с той, которую имел в виду Ферма. В любом случае она очень легко доказывает оба утверждения.

Так как  $p$  и  $q$  имеют противоположную четность, то числа  $p - q = s^2$ ,  $p + q = r^2$  нечетны; следовательно, нечетны и  $r$ ,  $s$ . Кроме того,  $r$  и  $s$  взаимно просты, поскольку, как показано выше, взаимно просты  $p - q$  и  $p + q$ . Определим положительные целые числа  $u$  и  $v$  равенствами

$$u = \frac{r-s}{2}, \quad v = \frac{r+s}{2}.$$

Тогда  $u$  и  $v$  взаимно просты; действительно, любой их общий делитель был бы общим делителем их суммы и разности  $r = u + v$ ,  $s = v - u$ , но  $r$  и  $s$  взаимно просты. Кроме того,

$$uv = \frac{r^2 - s^2}{4} = \frac{(p+q) - (p-q)}{4} = \frac{q}{2}.$$

Поскольку  $q$  является квадратом,  $\frac{1}{2}q$  может быть целым числом только тогда, когда оно будет четным целым. Следовательно,  $\frac{1}{2}uv = \frac{1}{4}q$  — целое, и это число является квадратом как отношение двух квадратов. Тогда либо  $u$ , либо  $v$  должно быть четным (поскольку  $\frac{1}{2}uv$  — целое), но не оба одновременно (так как они взаимно просты). Но половина четного из этих чисел взаимно проста с нечетным, а их произведение  $\frac{1}{2}uv$  является квадратом; поэтому сами множители должны быть квадратами, и, следовательно, четное из этих чисел является удвоенным квадратом, а нечетное — квадратом. Таким образом, равенство  $r = u + v$  дает, как и требовалось, представление  $r$  в виде суммы квадрата и удвоенного квадрата. Кроме того,

$$u^2 + v^2 = \frac{r^2 - 2rs + s^2}{4} + \frac{r^2 + 2rs + s^2}{4} = \frac{r^2 + s^2}{2} = \frac{(p+q) + (p-q)}{2} = p.$$

Таким образом,  $u^2 + v^2$  является квадратом, и оба утверждения Ферма доказаны.

За оставшейся частью доказательства проследить легко. Пифагорова тройка со «сторонами»  $u$ ,  $v$  примитивна, поскольку  $u$ ,  $v$  взаимно просты; следовательно, она имеет вид  $2PQ$ ,  $P^2 - Q^2$ ,  $P^2 + Q^2$ , где  $P$  и  $Q$  — взаимно простые числа противоположной

четности и  $P > Q$ . Так как  $\frac{1}{2}uv = PQ(P^2 - Q^2)$  является квадратом, то, как и раньше, отсюда следует, что все числа  $P$ ,  $Q$ ,  $P - Q$  и  $P + Q$  должны быть квадратами. Но

$$P + Q \leq (P + Q)PQ(P - Q) = \frac{1}{2}uv = q/4 < q < p + q,$$

и этот процесс можно повторить и найти еще два квадрата  $P'$ ,  $Q'$ , таких, что  $P' - Q'$  и  $P' + Q'$  также являются квадратами и  $P' + Q' < P + Q$ . Этот процесс может быть продолжен бесконечно; он даст бесконечно убывающую последовательность  $p + q > P + Q > P' + Q' > \dots$ . Поскольку такой бесконечный спуск невозможен, то пифагоров треугольник не может иметь площадь, равную квадрату.

Интересно, что это единственное дошедшее до нас доказательство Ферма доказывает также Последнюю теорему при  $n = 4$ . Действительно, оно показывает, что  $z^4 - x^4$  не может быть даже квадратом, не говоря уже о четвертой степени (см. упр. 2). Однако неразрешимость уравнения  $x^4 + y^4 = z^4$  можно доказать значительно проще методом предыдущего параграфа, и есть все основания полагать, что Ферма знал это более простое доказательство.

## Упражнения

1. Докажите, что если  $Ad^2$  — квадрат, то и  $A$  — квадрат.
2. Докажите, что уравнение  $x^4 - y^4 = z^2$  неразрешимо в ненулевых целых числах.

### 1.7. Суммы двух квадратов и родственные вопросы

Одной из первых задач в теории чисел, которую изучал Ферма, была задача представления чисел в виде сумм двух квадратов. Эта задача привела его ко многим другим важным вопросам. Как это часто случалось, интерес Ферма к этому предмету возник при чтении «Арифметики» Диофанта.

В книге Диофанта есть по крайней мере три места, связанные с представлениями в виде суммы двух квадратов; они показывают, что Диофант, бесспорно, хорошо знал этот предмет. В одном месте (III, 19) он замечает, что число 65 можно двумя способами записать в виде суммы двух квадратов:  $65 = 1^2 + 8^2 = 4^2 + 7^2$ , и объясняет это тем, что «65 является произведением чисел 13 и 5, каждое из которых равно сумме двух квадратов». В другом месте («необходимое условие» из V, 9) он фактически формулирует необходимое условие представимости данного числа в виде суммы двух квадратов; однако, как утверждает его переводчик и издатель Хит, «к несчастью, текст дополнительного условия неясен».

Наконец, в третьем месте (VI, 14) Диофант по ходу дела замечает, что число 15 не является суммой двух (рациональных) квадратов.

Основную роль в изучении чисел, которые являются суммами двух квадратов, играет формула

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \quad (1)$$

Она показывает, что если два числа представимы в виде суммы двух квадратов, то их произведение также будет суммой двух квадратов. Формула (1) является простым следствием коммутативного, ассоциативного и дистрибутивного законов, согласно которым обе ее части равны  $a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$ . Если двумя различными способами применить ее к  $5 = 2^2 + 1^2$  и  $13 = 3^2 + 2^2$ , то (как и утверждал Диофант) число  $65 = 5 \cdot 13$  можно будет двумя способами представить в виде суммы двух квадратов, а именно:  $65 = 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2) = (2 \cdot 3 - 1 \cdot 2)^2 + (2 \cdot 2 + 1 \cdot 3)^2 = 4^2 + 7^2$  и  $65 = 5 \cdot 13 = (2^2 + 1^2)(2^2 + 3^2) = (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2 = 1^2 + 8^2$ . В тринадцатом веке эта формула была известна Леонардо из Пизы (Фибоначчи); неявно она присутствует в алгебре древней Индии (см. далее § 1.9), и, конечно, в том или ином виде Диофант знал ее.

Ферма не был первым ученым, который попытался сделать ясными те места в книге Диофанта, где говорится о суммах двух квадратов. Такую же попытку, увенчавшуюся частичным успехом, предпринял Баше в своих комментариях к Диофанту. Другим комментатором был Франсуа Виет (1540—1603) — один из отцов-основателей современной алгебры. Третьим был Альбер Жирар (1595—1632), которому удалось дать необходимые и достаточные условия представимости данного числа в виде суммы двух квадратов за несколько лет до самых ранних известных нам записей Ферма по этому вопросу (см. Хит [Н1], стр. 106). Жирар, очевидно, считал квадратом  $0^2 = 0$ , и его условия состоят в том, что данное число можно представить в виде суммы двух квадратов тогда и только тогда, когда оно является (1) квадратом, или (2) простым числом, которое на 1 больше, чем некоторое кратное 4, или (3) числом 2, или (4) любым произведением таких чисел. Справедливость этих условий подтверждается таблицей 1.2, в которой приведены все числа, меньшие 250, которые можно представить в виде суммы двух квадратов. Неясно, опирался ли Жирар только на подобные эмпирические данные или действительно знал доказательство. Кажется, Жирар и не претендовал на то, что может доказать необходимость и достаточность своих условий.

Ферма же, с другой стороны, утверждал, что он может доказать необходимость и достаточность условий Жирара<sup>1)</sup>. Более

<sup>1)</sup> Нет оснований считать, что Ферма знал о работе Жирара. Он сформулировал эти условия независимо и несколько иным способом.

Таблица 1.2. Все числа, меньшие 256, которые являются суммами двух квадратов. Простые числа выделены жирным шрифтом

0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225
	<b>2</b>	<b>5</b>	10	<b>17</b>	26	<b>37</b>	50	65	82	<b>101</b>	122	145	170	<b>197</b>	226
		8	<b>13</b>	20	<b>29</b>	40	<b>53</b>	68	85	104	125	148	<b>173</b>	200	<b>229</b>
			18	25	34	45	58	<b>73</b>	90	<b>109</b>	130	153	178	205	234
				32	<b>41</b>	52	65	80	<b>97</b>	116	<b>137</b>	160	185	212	<b>241</b>
					50	<b>61</b>	74	<b>89</b>	106	125	146	169	194	221	250
						72	85	100	117	136	<b>157</b>	180	205	232	
							98	<b>113</b>	130	<b>149</b>	170	<b>193</b>	218	245	
								128	145	164	185	208	<b>233</b>		
									162	<b>181</b>	202	225	250		
										200	221	244			
												242			

трудная часть этой теоремы — доказательство *достаточности*. Поскольку  $a^2$ , очевидно, представляется в виде  $a^2 + 0^2$ , поскольку  $2 = 1^2 + 1^2$  и поскольку формула (1) показывает, что произведения сумм двух квадратов сами являются суммами двух квадратов, доказательство достаточности сводится к доказательству того, что *каждое простое число вида  $4n + 1$  можно записать как сумму двух квадратов*. Ферма неоднократно приводил формулировку этой теоремы и с полной определенностью утверждал, что может строго доказать ее, хотя, как обычно, неизвестно ни одной записи его доказательства. Ферма также пошел дальше Жирара, утверждая, что он может доказать *единственность* представления такого простого числа в виде суммы двух квадратов и что у него есть общий *метод* нахождения такого представления, не прибегающий к перебору. Доказательства этих теорем (возможно, те самые, которые имел в виду Ферма, а быть может, другие) приведены в § 2.4 и 2.6.

*Необходимость* условий Жирара можно переформулировать как утверждение о том, что *если частное от деления числа на наибольший содержащийся в нем квадрат делится на простое число вида  $4n + 3$ , то данное число нельзя представить в виде суммы двух квадратов*. Это также одна из теорем Ферма. Она значительно проще, чем вторая часть теоремы о представлении чисел в виде суммы двух квадратов, но ни в коем случае не тривиальна. (Доказательство этой теоремы см. в упр. 2 к § 1.8.)

Другой задачей, которую детально рассмотрел Ферма, была задача о нахождении *числа* представлений данного числа в виде суммы двух квадратов. Эта задача не имеет отношения к теме

нашей книги, и мы не будем рассматривать ее здесь, однако суть ее решения изложена в § 2.5.

Ферма обнаружил, что представления чисел в виде  $x^2 + 2y^2$  или  $x^2 + 3y^2$  управляются теми же законами, что и представления в виде сумм двух квадратов. Представления в виде  $x^2 + 2y^2$  не понадобятся при изучении Последней теоремы Ферма, и мы ограничимся здесь лишь кратким обзором относящихся к ним фактов. В табл. 1.3 приведены все числа, меньшие 256, которые можно представить в виде  $x^2 + 2y^2$ .

Таблица 1.3. Все числа, меньшие 256, которые можно представить в виде  $x^2 + 2y^2$ . Простые числа выделены жирным шрифтом

0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225
2	3	6	11	18	27	38	51	66	83	102	123	146	171	198	227
8	9	12	17	24	33	44	57	72	89	108	129	152	177	204	233
18	19	22	27	34	43	54	67	82	99	118	139	162	187	214	243
32	33	36	41	48	57	68	81	96	113	132	153	176	201	228	
50	51	54	59	66	75	86	99	114	131	150	171	194	219	246	
72	73	76	81	88	97	108	121	136	153	172	193	216	241		
98	99	102	107	114	123	134	147	162	179	198	219	242			
128	129	132	137	144	153	164	177	192	209	228	249				
162	163	166	171	178	187	198	211	226	243						
200	201	204	209	216	225	236	249								
242	243	246	251												

Изучение этой таблицы показывает, что, как и в предыдущем случае, входящие в эту таблицу числа можно описать как (1) квадраты, или (2) простые, которые входят в таблицу, или (3) любое произведение таких чисел. Следовательно, процедура, которая позволяет записать данное число в виде  $x^2 + 2y^2$ , должна состоять в том, чтобы записать его в виде квадрата, умноженного на произведение первых степеней простых чисел, и выяснить, представимы ли входящие в это произведение простые в виде  $x^2 + 2y^2$ . Если они представимы в таком виде, то аналог формулы (1), а именно

$$(a^2 + 2b^2)(c^2 + 2d^2) = (ac - 2bd)^2 + 2(ad + bc)^2$$

(обе части равны  $a^2c^2 + 2b^2c^2 + 2a^2d^2 + 4b^2d^2$ ), показывает, как записать исходное число в таком виде. Если хотя бы одно из них не представимо в виде  $x^2 + 2y^2$ , то по аналогии со случаем  $x^2 + y^2$  и как подсказывает таблица следует ожидать, что и само исходное число не представимо в виде  $x^2 + 2y^2$ . Для полной аналогии со случаем  $x^2 + y^2$  необходимо доказать эту теорему (если число, деленное на наибольший содержащийся в нем квадрат, имеет простой множитель, который не записывается в виде  $x^2 + 2y^2$ ,

то и само число не записывается в таком виде) и охарактеризовать все простые, которые представимы в виде  $x^2 + 2y^2$ . Ферма утверждал (и явно претендовал на то, что у него есть строгое доказательство), что *нечетное простое можно представить в виде  $x^2 + 2y^2$  тогда и только тогда, когда оно имеет вид  $8n + 1$  или  $8n + 3$* . Доказательство того, что простые числа, не имеющие вида  $8n + 1$  или  $8n + 3$ , не представимы в виде  $x^2 + 2y^2$ , — более легкая часть этой теоремы (см. упр. 3); обратное утверждение труднее (см. упр. 6 и 7 к § 2.4).

В отличие от представлений в виде  $x^2 + 2y^2$  представления в виде  $x^2 + 3y^2$  играют важную роль в изучении Последней теоремы, особенно в доказательстве Эйлера случая  $n = 3$ , поэтому аналогичные теоремы о таких представлениях будут подробно доказаны в следующей главе. В табл. 1.4 приведены все числа

Таблица 1.4. Все числа, меньшие 256, которые можно представить в виде  $x^2 + 3y^2$ . Простые числа выделены жирным шрифтом

0	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225
3	4	7	12	<b>19</b>	28	39	52	<b>67</b>	84	<b>103</b>	124	147	172	<b>199</b>	228
12	<b>13</b>	16	21	28	<b>37</b>	48	<b>61</b>	76	93	112	133	156	<b>181</b>	208	237
27	28	<b>31</b>	36	<b>43</b>	52	63	76	91	108	<b>127</b>	148	171	196	<b>223</b>	252
48	49	52	57	64	<b>73</b>	84	<b>97</b>	112	129	148	169	192	217	244	
75	76	<b>79</b>	84	91	100	111	124	<b>139</b>	156	175	196	219	244		
108	<b>109</b>	112	117	124	133	144	<b>157</b>	172	189	208	<b>229</b>	252			
147	148	<b>151</b>	156	<b>163</b>	172	183	196	<b>211</b>	228	<b>247</b>					
192	<b>193</b>	196	201	208	217	228	<b>241</b>								

вида  $x^2 + 3y^2$ , меньшие 256. Изучение этой таблицы показывает, что *опять данное число можно представить в виде  $x^2 + 3y^2$  тогда и только тогда, когда оно является (1) квадратом, или (2) простым числом такого вида, или (3) произведением таких чисел*. Далее, легко заметить, что все входящие в таблицу простые числа, кроме числа  $3 = 0^2 + 3 \cdot 1^2$ , которое явно является здесь исключительным, отличаются одно от другого на кратные 6, а на самом деле каждое из них на единицу больше, чем некоторое кратное 6. Поскольку *все простые* вида  $6n + 1$  рано или поздно окажутся в этой таблице (но не вообще все числа такого вида, так как отсутствует 55), то естественно догадаться, что *любое простое, отличное от 3, можно представить в виде  $x^2 + 3y^2$  тогда и только тогда, когда оно имеет вид  $6n + 1$* . Снова легко (см. упр. 2) доказать часть «только тогда» этой теоремы. Имеется аналог формулы (1), а именно

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2,$$

который делает очевидной часть «тогда» первой из приведенных теорем. Далее, каждое простое, отличное от 3, можно представить



в виде  $3n + 1$  или  $3n + 2$ , и простые числа вида  $3n + 1$  должны иметь вид  $6n + 1$ . Действительно, если  $n$  нечетно, то  $3n + 1$  четно и, следовательно, не может быть простым.

Эти наблюдения сводят две приведенные выше теоремы к следующим утверждениям: *если число, разделенное на наибольший содержащийся в нем квадрат, имеет простой делитель вида  $3n + 2$ , то его нельзя представить в виде  $x^2 + 3y^2$ ; каждое простое число вида  $3n + 1$  можно записать в виде  $x^2 + 3y^2$* . Эти теоремы доказываются в следующей главе.

Однако уже рассмотрение следующего случая показывает, что эти свойства представлений чисел в виде  $x^2 + y^2$ ,  $x^2 + 2y^2$ ,  $x^2 + 3y^2$  являются чем-то исключительным. Выражение  $x^2 + 4y^2$  является суммой двух квадратов, поэтому следующим случаем будет не  $x^2 + 4y^2$ , а  $x^2 + 5y^2$ . В табл. 1.5 приведены все числа,

Таблица 1.5. Все числа, меньшие 100, которые можно записать в виде  $x^2 + 5y^2$ . Простые числа выделены жирным шрифтом

0	1	4	9	16	25	36	49	64	81
<b>5</b>	6	9	14	21	30	<b>41</b>	54	69	86
20	21	24	<b>29</b>	36	45	56	69	84	
45	46	49	54	<b>61</b>	70	81	94		
80	81	84	<b>89</b>	96					

меньшие 100, которые представимы в виде  $x^2 + 5y^2$ . Заметим, что 21 встречается *дважды* (как  $1^2 + 5 \cdot 2^2$  и  $4^2 + 5 \cdot 1^2$ ), а его простые делители 3 и 7 не входят вообще. Это показывает, что в данном случае утверждения, подобные приведенным выше, не имеют места. Ферма высказал очень глубокую гипотезу о числах вида  $x^2 + 5y^2$ , которая свидетельствует о том, что он изучил эту задачу и осознал ее коренное отличие от предыдущих. Гипотеза Ферма состоит в том, что если два простых числа  $p_1$  и  $p_2$  оба имеют вид  $4n + 3$ , а их последняя цифра есть либо 3, либо 7, то  $p_1 p_2$  представимо в виде  $x^2 + 5y^2$ . (Простые 3, 7, 23, 43, 47, 67, . . . сравнимы с 3 по модулю 4 и оканчиваются на 3 или 7. Гипотеза состоит в том, что произведение любых двух этих чисел имеет вид  $x^2 + 5y^2$ . Например,  $3 \cdot 3 = 2^2 + 5 \cdot 1^2$ ,  $3 \cdot 7 = 4^2 + 5 \cdot 1^2$ ,  $7 \cdot 7 = 2^2 + 5 \cdot 3^2$ ,  $3 \cdot 23 = 8^2 + 5 \cdot 1^2$ ,  $3 \cdot 43 = 2^2 + 5 \cdot 5^2$ ,  $7 \cdot 23 = 9^2 + 5 \cdot 4^2$  и т. д.) Эта гипотеза не только верна, но и является основным фактом о числах вида  $x^2 + 5y^2$  (см. упр. 1 к § 8.6). Это еще одно подтверждение гениальности Ферма именно в теории чисел.

Упражнения

- 1. Докажите, что если  $x^2 + y^2$  — нечетное простое число, то оно представимо в виде  $4n + 1$ .
- 2. Докажите, что если  $x^2 + 3y^2$  — простое, отличное от 3, то оно имеет вид  $6n + 1$ .

3. Докажите, что если  $x^2 + 2y^2$  — нечетное простое, то оно имеет вид либо  $8n + 1$ , либо  $8n + 3$ .

4. Докажите, что необходимость условия Жирара можно, как указано в тексте, переформулировать в виде утверждения о том, что если частное от деления числа на наибольший содержащийся в нем квадрат делится на простое вида  $4n + 3$ , то данное число нельзя записать как сумму двух квадратов.

5. Покажите, что из теоремы Жирара следует утверждение Диофанта, согласно которому нельзя найти такие *рациональные* числа  $x$  и  $y$ , что  $x^2 + y^2 = 15$ .

6. Докажите, что произведение двух чисел вида  $x^2 + 5y^2$  также имеет такой вид.

## 1.8. Совершенные числа и теорема Ферма

Изучение «совершенных чисел» берет свое начало в предистории теории чисел, когда числам приписывали некие магические свойства. Число называется «совершенным», если оно равно сумме своих собственных делителей. Например, число 6 совершенно, поскольку  $6 = 1 + 2 + 3$ . Современному математику это понятие уже не кажется ни слишком захватывающим, ни слишком интересным. Однако в течение многих веков оно пленяло и завораживало ученых. Дискуссия о совершенных числах велась в широком масштабе: от такой мистики, как утверждение Алкуина (735—804) из Йорка и Тура о том, что совершенством числа 6 объясняется сотворение мира за 6 дней, до более близких к науке попыток найти все совершенные числа. Во времена Ферма интерес к совершенным числам еще далеко не угас, и в конце 1630-х годов между Ферма, Мерсенном, Декартом, Френиклем и другими велась обширная переписка по поводу совершенных чисел и родственных вопросов.

Евклид в «Началах» показал (Книга IX, предложение 36), что если  $1 + 2 + 4 + \dots + 2^{n-1} = 2^n - 1$  — простое число, то число  $2^{n-1} (2^n - 1)$  совершенно. Например,  $3 = 1 + 2$  — простое, поэтому  $2 \cdot 3 = 6$  — совершенное;  $7 = 1 + 2 + 4$  — простое, поэтому совершенно  $2^2 \cdot 7 = 28$ . В современных обозначениях это утверждение доказывается очень просто. Действительно, если  $p = 2^n - 1$  — простое, то собственными делителями числа  $2^{n-1}p$  являются  $1, 2, 4, \dots, 2^{n-1}, p, 2p, 4p, \dots, 2^{n-2}p$ , и их сумма равна  $1 + 2 + 4 + \dots + 2^{n-1} + p(1 + 2 + 4 + \dots + 2^{n-2}) = p + p(2^{n-1} - 1) = 2^{n-1}p$ , что и требовалось доказать. Условие Евклида является *достаточным* для того, чтобы число было совершенным. Никакие примеры других совершенных чисел неизвестны. Декарт утверждал (а Эйлер доказал это утверждение), что совершенное число имеет евклидов вид тогда (и, конечно, только тогда), когда оно четно. [Читателю предлагается доказать эту теорему в качестве упражнения.] Вопрос о том, существуют ли нечетные совершенные числа, является знаменитой нерешенной проблемой. К счастью, здесь мы можем без нее обойтись.



Согласно условию Евклида, для нахождения совершенных чисел достаточно <sup>1)</sup> найти простые числа в последовательности 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, . . . . Эта последняя задача уже представляет для нас значительный интерес. Короче говоря, *для каких значений  $n$  число  $2^n - 1$  является простым?* Решая эту задачу, Ферма сделал важное открытие, известное теперь как теорема Ферма.

Во-первых, числа 15, 63, 255, 1023 ( $= 3 \cdot 341$ ), 4095, очевидно, не являются простыми. Вообще, если  $n$  четно и больше 2, то  $2^n - 1 = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$  — не простое. Нечетные значения  $n = 3, 5, 7$  приводят к простым 7, 31, 127, но нечетное значение  $n = 9$  дает 511 и, как легко видеть, 511 делится на 7. Это приводит к предположению, что если  $n$  — не простое, то число  $2^n - 1$  также не является простым. Это предположение легко проверяется, если заметить, что  $2^{km} - 1 = (2^k - 1) \times (2^{k(m-1)} + 2^{k(m-2)} + \dots + 2^k + 1)$ . Последнее замечание сводит рассматриваемый вопрос к вопросу о том, *для каких простых  $p$  число  $2^p - 1$  является простым.* Простые числа вида  $2^p - 1$  называются *простыми Мерсенна* в честь постоянного корреспондента Ферма преподобного Марэна Мерсенна (1588—1648).

Простым 2, 3, 5, 7 соответствуют простые Мерсенна 3, 7, 31, 127 (и, следовательно, совершенные числа 6, 28, 496, 8128). Проверим, является ли простым  $2^{11} - 1$ . На этот вопрос легко ответить, найдя число  $2^{11} - 1 = 2047$  в явном виде и пробуя делить его на все простые, меньшие  $\sqrt{2047}$ , чтобы узнать, делит ли какое-нибудь из них 2047 нацело. Однако поучительнее подойти к этой задаче другим способом, который можно использовать затем для больших, чем 11, показателей  $p$ .

Посмотрим, делится ли  $2^{11} - 1$  на 7. Представим себе, что степени числа 2 записаны в одну строку, а под ними записаны их остатки при делении на 7:

степени числа 2	1	2	4	8	16	32	64	128	256	512...
остатки	1	2	4	1	2	4	1	2	4	1...

Закономерность в расположении остатков очевидна, и ясно, что остаток от деления  $2^n$  на 7 равен 1 тогда и только тогда, когда  $n$  делится на 3, т. е. *7 делит  $2^n - 1$  тогда и только тогда, когда 3 делит  $n$ .* Следовательно, 7 не делит  $2^{11} - 1$ . Тот же метод можно использовать и для других простых. Некоторые результаты приведены в табл. 1.6. Ясно, что для каждого простого  $p$  остатки расположены в циклическом порядке и *существует такое целое  $d$ , что  $p$  делит  $2^n - 1$  тогда и только тогда, когда  $d$  делит  $n$ .* Как

<sup>1)</sup> Смешение необходимых и достаточных условия — кажется, основная слабость человеческого интеллекта. Даже Ферма утверждал, что не существует совершенных чисел, состоящих из 20 или 21 цифры, имея в виду, что не существует таких чисел *евклидова типа*.

Таблица 1.6

$p = 3$	1	2	4	8	16	32	64	...								$d = 2$	
	1	2	1	2	1	2	1	...									
$p = 5$	1	2	4	8	16	32	64									$d = 4$	
	1	2	4	3	1	2	4	...									
$p = 11$	1	2	4	8	16	32	64	128	256	512	1024	2048	...			$d = 10$	
	1	2	4	8	5	10	9	7	3	6	1	2	...				
$p = 13$	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	...		$d = 12$
	1	2	4	8	3	6	12	11	9	5	10	7	1	2	...		
$p = 17$	1	2	4	8	16	32	64	128	256	512	1024	2048	...			$d = 8$	
	1	2	4	8	16	15	13	9	1	2	4	8	...				

только этот факт замечен, его легко доказать. Поскольку при делении на  $p$  возможны только  $p - 1$  остатков, в последовательности остатков по крайней мере два остатка должны совпадать; пусть, скажем, числа  $2^n$  и  $2^{n+m}$  имеют один и тот же остаток. Тогда  $p$  делит их разность  $2^{n+m} - 2^n = 2^n (2^m - 1)$ , но  $p$  — простое число и не делит 2, следовательно,  $p$  делит  $2^m - 1$ . Поэтому остаток от деления числа  $2^m$  на  $p$  равен 1. Следовательно, число 1 входит в последовательность остатков. Пусть  $2^d$  — наименьшая степень числа 2, которая дает в остатке 1. Тогда  $2^{md}$  при делении на  $p$  также дает в остатке 1, поскольку  $2^{md} - 1 = (2^d - 1) \times (2^{(m-1)d} + \dots + 2^d + 1)$  делится на  $p$ . Обратно, единственными степенями числа 2, которые дают в остатке 1, являются степени, соответствующие кратным  $d$ . Действительно, если  $2^m$  дает в остатке 1 и если  $m = qd + r$  ( $q \geq 0, 0 \leq r < d$ ), то как  $2^m = 2^{qd} 2^r$ , так и  $2^{qd}$  дают в остатке 1, и их разность  $2^{qd} (2^r - 1)$  делится на  $p$ . Так как  $2^{qd}$  не делится на  $p$ , то это противоречит определению  $d$  (напомним, что  $0 \leq r < d$ ), за исключением случая, когда  $r = 0$  и  $m$  кратно  $d$ , что и требовалось доказать. Кроме того, выше мы заметили, что  $2^{n+m}$  и  $2^n$  дают одинаковые остатки только тогда, когда  $2^m$  дает в остатке 1, т. е. остатки повторяются только через интервалы, длина которых делится на  $d$ . Следовательно, существует в точности  $d$  различных остатков и они циклически повторяются, как и в рассмотренных примерах.

Из этого замечания об остатках следует, что если мы хотим определить, делится ли  $2^{11} - 1$  на  $p$ , достаточно найти соответствующее значение  $d$  и выяснить, делится ли 11 на  $d$ . Поскольку 11 — простое число, последнее условие равносильно тому, что  $d = 11$ . Для всех рассмотренных до сих пор простых ответ на этот вопрос отрицателен.

Существует более простой способ нахождения последовательности остатков, который не требует прямого вычисления  $2^n$  и деления его на  $p$  (для  $n = 1, 2, 3, \dots$ ). Например, поскольку

известно, что при делении 128 на 13 получается остаток 11, то остаток от деления 256 на 13 легко найти путем удвоения 11 и вычитания 13 из полученного результата; таким образом, следующий остаток равен  $22 - 13 = 9$ . Далее получится остаток  $2 \cdot 9 - 13 = 5$ , а за ним  $2 \cdot 5$ . Вообще, каждый остаток равен либо удвоенному предыдущему, либо удвоенному предыдущему минус  $p$  и любой из них лежит в области значений остатков  $1 \leq r \leq p - 1$ . Действительно, если  $2^n - r$  делится на  $p$ , то  $2^{n+1} - 2r$  делится на  $p$ , и отсюда немедленно следует, что  $2^{n+1}$  и  $2r$  имеют один и тот же остаток при делении на  $p$ . Таким образом, для  $p = 19$  остатками являются 1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1, 2, 4, ..., поэтому  $d = 18 \neq 11$ ; следовательно,  $2^{11} - 1$  не делится на 19. Для следующего простого  $p = 23$  получаются остатки 1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1, 2, 4, ...; отсюда следует, что  $d = 11$  и 23 делит  $2^{11} - 1$ . Таким образом,  $2^{11} - 1$  не является простым, и действительно,  $2^{11} - 1 = 2047 = 23 \cdot 89$ .

Аналогичным образом можно подойти к задаче, является ли простым число  $2^{13} - 1$  (а тем самым является ли совершенным  $2^{12} (2^{13} - 1)$ ). Мы должны выяснить, существует ли простое  $p$ , для которого  $d = 13$ . Все рассмотренные до сих пор простые можно исключить (поскольку соответствующие им  $d$  оказались отличными от 13), и нам остается проверить, равно ли  $d$  числу 13 для  $p = 29, 31, 37, \dots$  до последнего простого, которое меньше чем  $\sqrt{2^{13} - 1} = \sqrt{8191} < 91$ . Ферма заметил одну несложную закономерность в значениях  $d$ , которая позволяет немедленно исключить из рассмотрения все, кроме очень небольшого числа таких простых. Попробуйте обнаружить ее самостоятельно! Вот несколько первых значений  $d$ :

$p$	3	5	7	11	13	17	19	23	29	31	37
$d$	2	4	3	10	12	8	18	11	28	5	36

Конечно, поскольку  $d$  — число различных остатков,  $d$  не превосходит  $p - 1$ . Ферма заметил, что на самом деле  $d$  делит  $p - 1$ . Отсюда следует, что  $d$  может равняться 13, только если 13 делит  $p - 1$ . Поэтому возможными значениями  $p$  являются  $13 + 1, 26 + 1, 39 + 1, 52 + 1, \dots$ . Из них только нечетные числа  $27, 27 + 26 = 53, 53 + 26 = 79, \dots$  могут быть простыми. Поскольку 27 не является простым, а  $79 + 26$  больше чем  $\sqrt{2^{13} - 1}$ , то это означает, что нужно испытать *только два* простых, а именно: 53 и 79. Соответствующие им значения  $d$ , которые определяются использованным выше методом, равны 52 и 39. Таким образом, если мы убеждены в том эмпирическом факте, что  $d$  делит  $p - 1$ , то из этих кратких вычислений мы сразу получаем, что  $2^{13} - 1 = 8191$  — простое число.

Учитывая, что  $d$  делит  $m$  тогда и только тогда, когда  $2^m - 1$  делится на  $p$  (см. выше), мы можем утверждение о том, что  $d$  делит  $p-1$ , переформулировать в виде « $p$  делит  $2^p-1-1$ », или « $p$  делит  $2^p - 2$ ». Ферма формулирует свою теорему как в последнем виде, так и в виде  $d \mid (p - 1)$ <sup>1)</sup>. Как обычно, Ферма утверждает, что у него есть доказательство этой теоремы, но опускает его. Возможно, его доказательство было следующим.

Согласно определению, существуют в точности  $d$  возможных остатков  $1, 2, 3, \dots, p - 1$ , которые могут встретиться при делении степеней 2 на  $p$ . Если каждый из них встречается на самом деле, то  $d = p - 1$  и требуемое заключение  $d \mid (p - 1)$  справедливо. В противном случае среди них найдется хотя бы одно число  $k$ , не попадающее в число остатков. Среди возможных остатков  $1, 2, 3, \dots, p - 1$  рассмотрим те, которые получаются при делении на  $p$  чисел вида  $k, 2k, 4k, 8k, \dots, 2^n k, \dots$ . Таких остатков в точности  $d$ , и ни один из них не входит в исходное множество из  $d$  остатков. Первое из этих двух утверждений следует из того, что  $2^{n+m}k$  и  $2^n k$  дают один и тот же остаток тогда и только тогда, когда  $2^n k (2^m - 1)$  делится на  $p$ , а это верно в том и только в том случае, когда  $m$  делится на  $d$ . Для доказательства второго достаточно заметить, что если бы  $2^n$  и  $2^m k$  давали один и тот же остаток, то тем же свойством обладали бы  $2^{n+1}$  и  $2^{m+1}k$  (поскольку  $2^n - 2^m k$  делится на  $p$  тогда и только тогда, когда  $2(2^n - 2^m k)$  делится на  $p$ ), а также  $2^{n+2}$  и  $2^{m+2}k$ , и т. д.; отсюда следует (если выбрать  $m + j$  делящимся на  $d$ ), что  $2^{n+j}$  и  $k$  при делении на  $p$  дают один и тот же остаток, а это противоречит выбору  $k$ . Если эти два множества остатков исчерпывают все  $p - 1$  возможных остатков, то  $p - 1 = 2d$  и  $d \mid (p - 1)$ , что и требовалось доказать. В противном случае найдется еще один возможный остаток  $k'$ , который не принадлежит ни тому ни другому множеству. Тогда, так же как и раньше, остатки чисел  $k', 2k', 4k', \dots, 2^n k', \dots$  образуют множество, состоящее еще из  $d$  различных остатков, ни один из которых не принадлежит никакому из двух уже найденных множеств. Продолжив этот процесс, мы разобьем множество всех  $p - 1$  возможных остатков на подмножества, каждое из которых состоит из  $d$  элементов. Отсюда, конечно, следует, что  $d$  обязательно делит  $p - 1$ , что и требовалось доказать.

Например, при  $p = 31$  степени 2 дают остатки  $1, 2, 4, 8, 16$ . В этот список не входит 3, и числа  $3, 2 \cdot 3, 4 \cdot 3, 8 \cdot 3, \dots$  дают остатки  $3, 6, 12, 24, 17$ . Ни один из этих списков не включает 5; при делении чисел  $5, 2 \cdot 5, 4 \cdot 5, 8 \cdot 5, \dots$  в остатке получаются  $5, 10, 20, 9, 18$ . Если продолжить таким образом, то остатки  $1, 2, \dots$

<sup>1)</sup> Вертикальная черта означает «делит», и  $d \mid (p - 1)$  читается как « $d$  делит  $p - 1$ ». Перечеркнутая вертикальная черта  $\nmid$  означает «не делит».

... , 30 сгруппируются в шесть множеств из пяти элементов: три перечисленных выше и множества (7, 14, 28, 25, 19), (11, 22, 13, 26, 21), (15, 30, 29, 27, 23). Тот факт, что  $p - 1$  остатков всегда распадаются таким образом на множества из  $d$  элементов, гарантирует, что  $d$  всегда делит  $p - 1$ .

Ни одно из этих рассуждений не зависит от каких-либо специальных свойств числа 2, которое было выбрано только потому, что оно появляется в связи с нахождением совершенных чисел, и для любого другого положительного целого  $a$  те же самые рассуждения доказывают такую теорему: если  $p$  — простое, которое не делит  $a$ , то существует такое целое  $d$ , что  $p$  делит  $a^m - 1$  тогда и только тогда, когда  $d$  делит  $m$ . Теорема Ферма утверждает, что  $d$  делит  $p - 1$ . Согласно определяющему свойству  $d$ , это утверждение сводится к тому, что  $p$  делит  $a^{p-1} - 1$ , или, что то же самое, что  $p$  делит  $a^p - a$ . Последнее утверждение самое краткое, поскольку в него вообще не входит  $d$  и поскольку оно справедливо, даже если  $p$  делит  $a$ . Это обычная формулировка теоремы Ферма: *если  $p$  — простое число и  $a$  — произвольное целое, то  $p$  делит  $a^p - a$ .*

Теорема Ферма — одно из самых важных арифметических свойств целых чисел; мы будем существенно пользоваться ею в последующих главах этой книги. Остальная часть данного параграфа, напротив, посвящена вопросу, который представляет лишь исторический интерес. Это вопрос о так называемых *числах Ферма*  $2^1 + 1$ ,  $2^2 + 1$ ,  $2^4 + 1$ ,  $2^8 + 1$ ,  $2^{16} + 1$ ,  $2^{32} + 1$ , ... . В переписке Ферма неоднократно выражал свое убеждение в том, что все эти числа — *простые*. (Заметим, что  $2^n + 1$  не является простым, если  $n$  не есть степень двойки; действительно, если  $n$  имеет нечетный делитель  $k$ , например  $n = km$ , то  $2^n + 1 = (2^m + 1) \cdot (2^{m(k-1)} - 2^{m(k-2)} + \dots + 2^{2m} - 2^m + 1)$ .) Таким образом, он полагал, что решил древнюю задачу нахождения формулы, которая дает сколь угодно большие простые числа. В конце жизни Ферма даже заявил <sup>1)</sup>, что может *доказать* простоту всех таких чисел.

Несколько первых чисел Ферма — простые. Числа  $2^1 + 1 = 3$ ,  $2^2 + 1 = 5$  и  $2^4 + 1 = 17$ , несомненно, простые. Простоту  $2^8 + 1 = 257$  можно доказать следующим образом. Если  $p$  делит  $2^8 + 1$ , то оно делит  $(2^8 + 1)(2^8 - 1) = 2^{16} - 1$ . Следовательно, соответствующее ему  $d$  (при  $a = 2$ ) должно делить 16. Но делителями 16 являются только 1, 2, 4, 8, 16, и  $d$  не может равняться 1, 2, 4 или 8, поскольку в этом случае  $p$  делило бы  $2^8 - 1$ , а это противоречит предположению, что  $p$  делит  $2^8 + 1$ . Следовательно,  $d = 16$  и по теореме Ферма  $p = 16n + 1$  для некоторого целого  $n$ .

<sup>1)</sup> Э. Т. Белл ([B1], стр. 256) настаивает на том, что Ферма никогда не делал такого заявления. Я не вижу другой интерпретации его письма Каркави [F5].

Но наименьшее такое простое  $p = 17$  уже больше чем  $\sqrt{2^8 + 1}$ , и  $2^8 + 1$  не имеет собственных делителей, что и требовалось доказать.

Аналогично, единственными простыми делителями  $2^{16} + 1$  могут быть только простые вида  $p = 32n + 1$ . Поскольку  $\sqrt{2^{16} + 1}$  лишь немного больше чем  $2^8 = 256$ , то мы должны испытать только простые числа в списке 33, 65, 97, 129, 161, 193, 225, в котором лишь два простых 97, 193. Ни одно из них не делит  $2^{16} + 1$ , поскольку остатки, которые получаются при делении степеней  $1, 2, 4, 8, 16, \dots, 2^{16}$  на 97, равны 1, 2, 4, 8, 16, 32, 64, 31, 62, 27, 54, 11, 22, 44, 88, 79, 61, так что при делении  $2^{16} + 1$  на 97 получается в остатке 62, а остатки при делении этих степеней на 193 равны 1, 2, 4, 8, 16, 32, 64, 128, 63, 126, 59, 118, 43, 86, 172, 151, 109, и при делении  $2^{16} + 1$  на 193 в остатке получается 110. Следовательно,  $2^{16} + 1$  — простое число.

Аналогичное доказательство для  $2^{32} + 1$  гораздо длиннее, и Ферма, должно быть, не пытался всерьез его провести либо допустил ошибку в вычислениях. Согласно такому же рассуждению, как и выше, единственными простыми делителями  $2^{32} + 1$  могут быть числа вида  $p = 64n + 1$ . Если  $2^{32} + 1$  не является простым, то его наименьший простой делитель не может быть больше чем  $2^{16}$ . Поскольку числа  $64n + 1$  расположены через интервалы в  $64 = 2^6$  единицы, грубо говоря, надо проверить  $2^{10} = 1024$  числа. Однако каждое третье из них делится на 3, каждое пятое — на 5, и т. д.; поэтому количество *простых*  $p = 64n + 1$ , лежащих в критической области, только порядка 500 или в этом роде. Доказывать таким способом, что  $2^{32} + 1$  — простое число, — довольно долгое дело, хотя оно и займет не больше нескольких дней. Однако число  $2^{32} + 1$  *не является* простым; оно делится на 641. Если следовать описанной выше процедуре, то мы должны проверить последовательно 193, 257, 449, 577, а затем 641. Таким образом, 641 — всего лишь *пятое* <sup>1)</sup> простое число, которое следует проверить. Делитель 641 числа  $2^{32} + 1$  был обнаружен Эйлером.

Эта неудача, кажется, — единственное серьезное пятно на репутации Ферма как специалиста по теории чисел. Дело усугубляется тем, что, как нам теперь известно, следующие несколько чисел Ферма:  $2^{64} + 1$ ,  $2^{128} + 1$ ,  $2^{256} + 1$  и несколько других — *все* составные. Не найдено *ни одного* простого числа Ферма за пределами  $2^{16} + 1$ . Однако даже здесь есть смягчающее обстоятельство, еще одно подтверждение безошибочного инстинкта Ферма при выборе задачи. Через полтора века после того, как Ферма выдвинул свою гипотезу, юный Гаусс показал, что евклидово построение пятиугольника при помощи циркуля и линейки тесно связано

<sup>1)</sup> Улучшение этого рассуждения см. в упр. 10 к § 2.4.



с тем фактом, что  $5 = 2^2 + 1$  является числом Ферма. Вообще, Гаусс доказал, что если  $n$  — простое число Ферма, то правильный  $n$ -угольник можно построить при помощи циркуля и линейки. Обратно, как утверждал Гаусс и доказал Ванцель (см. [К1а]), при помощи циркуля и линейки можно построить только те правильные  $n$ -угольники, для которых  $n = 2^k p_1 p_2 \dots p_m$ , где  $p_1, p_2, \dots, p_m$  — различные простые числа Ферма и  $k \geq 0$ .

## Упражнения

1. Докажите, что число  $2^{37} - 1$  не является простым. [При проверке данного простого не обязательно находить  $d$ ; достаточно определить, делит ли это простое  $2^{37} - 1$ . Для этого не надо находить остатки, получающиеся при делении всех чисел  $1, 2, 4, 8, 16, \dots$ , так как достаточно найти только те остатки, которые получаются при делении чисел  $2, 2^2, 2^4, 2^8, 2^{16}, 2^{32}, 2^{32+4}, 2^{37}$ .]

2. Докажите, что число, которое не удовлетворяет условиям Жирара, нельзя представить в виде суммы двух квадратов. Точнее, докажите, что если  $p$  делит  $x^2 + y^2$  и  $p$  — простое вида  $4n + 3$ , то  $p$  делит как  $x$ , так и  $y$ . [Если  $p$  делит  $x^2 + y^2$ , то оно делит число  $(x^2)^{2n+1} + (y^2)^{2n+1}$ . Если же  $p$  не делит хотя бы одно из  $x, y$ , то это число на 1 или 2 больше чем некоторое кратное  $p$  и, следовательно, не может делиться на  $p$ .]

3. Покажите, как можно построить правильный треугольник при помощи циркуля и линейки. Рассмотрите евклидово построение правильного пятиугольника («Начала», Книга IV, предложение 11). Покажите, как, используя эти два построения, можно построить правильный 15-угольник. Применяя теорему Гаусса и Ванцеля, найдите все такие значения  $n \leq 30$ , что правильный  $n$ -угольник можно построить при помощи циркуля и линейки.

## 1.9. Уравнение Пелля

В 1657 г. — в довольно поздний период своей деятельности — Ферма в качестве вызова разослал другим математикам, в частности английским, одну задачу: он надеялся найти среди них кого-нибудь, кто разделял бы его интерес к теории чисел.

«Сейчас едва ли найдется кто-нибудь, кто предлагает арифметические вопросы, и кто-нибудь, кто их понимает. Не потому ли это происходит, что до сих пор арифметику рассматривали скорее с геометрической, чем с арифметической точки зрения? Так было всегда — и в древних, и в современных работах; примером тому является даже Диофант. Ибо хотя он и более чем другие освободился от геометрии в том отношении, что ограничивает свой анализ рассмотрением рациональных чисел, однако даже у него геометрия не полностью отсутствует, как достаточно доказала *Zetetica* Виета, где метод Диофанта распространяется на непрерывные величины и тем самым на геометрию.

Теперь арифметика имеет, так сказать, собственную область изучения — теорию целых чисел. Евклид лишь слегка затронул ее в своих «Началах», а его последователи недостаточно занимались этой теорией (если только она не содержалась в тех книгах Диофанта, которых мы лишились вследствие разрушительного действия времени); следовательно, арифметикам предстоит развивать или восстанавливать ее.

Поэтому арифметикам, дабы осветить тот путь, по которому надо следовать, предлагаю я эту теорему, чтобы они доказали ее, или эту задачу, чтобы они решили ее. Если же преуспеют они в ее доказательстве или решении, то им придется признать, что вопросы такого рода ничем не уступают в отношении красоты, трудности или метода доказательства самым знаменитым вопросам геометрии.

*Если дано произвольное число, которое не является квадратом, то найдется также и бесконечное количество таких квадратов, что если этот квадрат умножить на данное число и к произведению прибавить единицу, то результат будет квадратом.*

Пример. Пусть 3, которое не является квадратом, будет данным числом. Если умножить его на квадрат, равный 1, и к произведению добавить 1, то в результате получится 4, что является квадратом.

Если то же самое 3 умножить на квадрат 16, то получится произведение, которое при увеличении на 1 превращается в 49, тоже квадрат.

И кроме 1 и 16 можно найти бесконечное количество квадратов с тем же самым свойством.

Но я спрашиваю об общем правиле решения — когда дано произвольное число, не являющееся квадратом.

Например, требуется найти такой квадрат, что если произведение этого квадрата и числа 149, или 109, или 433 и т. д. увеличить на 1, то в результате получится квадрат». (Перевод на английский с латинского оригинала см. у Хита [Н1], стр. 285—286.)

Вступление Ферма к формулировке этой задачи ясно показывает, что он делает четкое различие между диофантовой традицией решения в рациональных числах и традицией, с которой он теперь ассоциирует самого себя, решения в *целых числах*. (По иронии судьбы в современной терминологии «диофантово» означает «целое», тогда как Диофант ни в одной дошедшей до нас части его работы не занимался решениями в целых числах.) Как это ни странно, вступление было опущено одним из посредников в том экземпляре письма, который был переправлен английским математикам; в результате они сочли эту задачу глупой, имеющей тривиальное диофантово решение

$$Ax^2 + 1 = y^2 \quad (\text{дано } A, \text{ найти } x, y),$$

$$y = 1 + \frac{m}{n}x \quad (\text{например}),$$

$$Ax^2 + 1 = 1 + \frac{2m}{n}x + \frac{m^2}{n^2}x^2,$$

$$An^2x^2 - m^2x^2 = 2mnx,$$

$$x = \frac{2mn}{An^2 - m^2}, \quad y = \frac{An^2 + m^2}{An^2 - m^2},$$

которое дает бесконечно много рациональных ответов. Когда же дополнительное требование, что  $x$  и  $y$  должны быть целыми числами, дошло до них, они обнаружили, что это «решение» не имеет никакой ценности, и пожаловались, что Ферма изменил условие задачи. Конечно, их жалоба оправдана в свете сильной диофанто-

вой традиции, но, как указал Ферма, с их стороны было наивно полагать, что он предложил столь тривиальную задачу.

Конечно, Ферма не был первым, кто начал изучать свойства целых чисел. В тех книгах «Начал» Евклида, которые посвящены арифметике, рассматриваются исключительно целые числа; Платон тоже неоднократно говорил о предпочтительности с философской точки зрения изучения целых чисел. Но Ферма возродил эту древнюю традицию и пытался при помощи своей задачи пробудить в других такой же интерес. Поскольку ему не удалось заинтересовать сограждан — например Паскаля — своими занятиями арифметикой целых чисел, теперь он был готов войти в международную переписку, пытаясь найти других ученых, которые разделяли бы его интересы.

Мотивировка задачи: «доказать, что для данного положительного целого  $A$ , не являющегося квадратом, найдется бесконечно много целых  $x$ , для которых  $Ax^2 + 1$  является квадратом» — лежит в собственных работах Ферма, а так как Ферма был очень скрытным во всем, что касалось его математической деятельности, то теперь невозможно реконструировать тот путь, который привел его к этой задаче. В какой-то мере эта задача неявно присутствует в некоторых местах у Диофанта (см. Диксон [D2], т. 2, стр. 345—346), и довольно ясно, что некоторые задачи Диофанта и комментарии Баше к ним привели Ферма к задачам, которые включали целочисленные решения квадратных уравнений с двумя неизвестными, но детали этой связи непонятны. С определенностью можно лишь сказать, что эта задача была выбрана не случайно. Как обнаружили позднейшие исследования, это частное квадратное уравнение в целых числах  $y^2 - Ax^2 = 1$  играет важную роль в решении произвольных квадратных уравнений с двумя неизвестными в целых числах.

Конечно, Ферма не был первым, кто распознал важность этой задачи. Есть указания на то, что интерес к ней проявляли еще древнегреческие математики — об этом свидетельствует пифагорово решение <sup>1)</sup> для случая  $A = 2$ , связанное с иррациональностью  $\sqrt{2}$ , а в немотивированном утверждении Архимеда, что  $1351/780 > \sqrt{3}$ , проявляется знание решения  $3 \cdot 780^2 + 1 = 1351^2$  задачи Ферма при  $A = 3$ . Многие историки полагали, что древние греки обладали значительными знаниями этого предмета, которые не дошли до нас. Доказательства интереса, проявляемого к этой зада-

---

<sup>1)</sup> Это решение можно получить из формулы  $(a^2 - 2b^2)(c^2 - 2d^2) = (ac + 2bd)^2 - 2(ad + bc)^2$  и равенства  $1^2 - 2 \cdot 1^2 = -1$ . Действительно,  $1 = (-1)(-1) = (1^2 - 2 \cdot 1^2)(1^2 - 2 \cdot 1^2) = 3^2 - 2 \cdot 2^2$ ,  $-1 = (-1) \cdot 1 = (1^2 - 2 \cdot 1^2)(3^2 - 2 \cdot 2^2) = 7^2 - 2 \cdot 5^2$ ,  $1 = (1^2 - 2 \cdot 1^2)(7^2 - 2 \cdot 5^2) = 17^2 - 2 \cdot 12^2$ , и т. д.;  $n$ -е равенство дает  $d_n^2 - 2 \cdot s_n^2 = (-1)^n$ , где  $d_n = d_{n-1} + 2s_{n-1}$  и  $s_n = d_{n-1} + s_{n-1}$ . Равенства с четными номерами дают решения  $s_{2k}$  задачи Ферма: « $2 \cdot s_{2k}^2 + 1$  является квадратом». См. Диксон [D2, т. 2, стр. 341].

че в древней Индии, документированы полнее. (См. [D2], т. 2, стр. 346—350, [C3] или [H1], стр. 281—285.) В очень давние времена (за несколько веков до н. э.) в древней Индии было известно решение  $2 \cdot 408^2 + 1 = 577^2$ , а решение  $92 \cdot 120^2 + 1 = 1151^2$ , являющееся наименьшим в случае  $A = 92$ , вместе с изощренной техникой его вывода было получено Брахмагуптой (родился в 598 г. н. э.). Общий способ решения этого уравнения (так называемый «циклический метод») дал Бхаскара Акхария (родился в 1114 г. н. э.). Сущность этого метода состоит в следующем.

Предположим, что  $A = 67$ , т. е. задача состоит в том, чтобы найти такое целое  $x$ , что  $67x^2 + 1$  является квадратом, или, что то же самое, найти такие целые  $x$  и  $y$ , что  $y^2 - 67x^2 = 1$ . Поскольку  $8^2 - 67 \cdot 1^2 = -3$  достаточно близко к 1, в качестве первого приближения к таким числам  $x$  и  $y$  можно взять 1, 8. Рассмотрим теперь аналог формулы (1) из § 1.7 для этого случая, а именно формулу

$$(a^2 - 67b^2)(c^2 - 67d^2) = (ac + 67bd)^2 - 67(ad + bc)^2.$$

Применив ее к равенствам  $8^2 - 67 \cdot 1^2 = -3$  и  $r^2 - 67 \cdot 1^2 = s$  (где  $r$ , а тем самым и  $s$  должны быть определены позже), мы получим, что

$$(8r + 67)^2 - 67(r + 8)^2 = -3s.$$

Попытка сделать это число как можно меньше только за счет выбора наименьшего возможного  $s$  привела бы к выбору  $r = 8$ ,  $s = -3$ , и мы получили бы  $131^2 - 67 \cdot 16^2 = 9$ . Ясно, что это никуда не ведет. «Циклический метод» состоит в том, чтобы *выбрать  $r$  таким образом, что  $r + 8$  делится на 3*, и в то же время сделать  $s$  возможно меньшим. Когда это сделано, последнее уравнение показывает, что  $8r + 67$  должно делиться на 3 и, следовательно, левая часть этого уравнения должна делиться на  $3^2$ . Таким образом,  $s$  должно делиться на 3, и обе части уравнения должны делиться на 9. Это приводит к существенно новому случаю, в котором  $y^2 - 67x^2$  является маленьким числом.

Проведем эти рассуждения явно. Для того чтобы  $r + 8$  делилось на 3,  $r$  должно принимать одно из значений 1, 4, 7, 10, 13, .... Выбор  $r = 7$ ,  $s = -18$  дает наименьшее (по абсолютной величине)  $s$ ; этим  $r$  и  $s$  соответствует равенство  $123^2 - 67 \cdot 15^2 = 54$ , которое после сокращения на 9 превращается в

$$41^2 - 67 \cdot 5^2 = 6.$$

Теперь этот процесс можно повторить. Умножая обе части последнего равенства на  $r^2 - 67 \cdot 1^2 = s$ , получим  $(41r + 67 \cdot 5)^2 - 67(5r + 41)^2 = 6s$ . Если, как и раньше, выбрать такое  $r$ , что  $5r + 41$  делится на 6, то мы сможем обе части уравнения сократить на  $6^2$ . Для того чтобы  $5r + 41$  делилось на 6, необходимо и достаточно, чтобы  $r + 1 = 6(r + 7) - (5r + 41)$  делилось на 6, что

справедливо при  $r = 5, 11, 17, 23, \dots$ . Выбор  $r = 5$  дает наименьшее значение  $s$ , и мы получаем  $540^2 - 67 \cdot 66^2 = 6 \cdot (-42)$ , что после сокращения на  $6^2$  превращается в

$$90^2 - 67 \cdot 11^2 = -7.$$

Конечно, не ясно, привела ли эта процедура нашу задачу хоть немного ближе к решению, но по крайней мере понятно, что ее продолжение может в конце концов привести к уравнению, правая часть которого, как и требуется, равна 1. В данной задаче дело обстоит именно так; продолжение процесса «циклического метода» в нашем случае дает ее решение:

$1^2 - 67 \cdot 0^2 =$	1	
$8^2 - 67 \cdot 1^2 =$	-3	$r = 8$
$41^2 - 67 \cdot 5^2 =$	6	$r = 7$
$90^2 - 67 \cdot 11^2 =$	-7	$r = 5$
$221^2 - 67 \cdot 27^2 =$	-2	$r = 9$
$1899^2 - 67 \cdot 232^2 =$	-7	$r = 9$
$3577^2 - 67 \cdot 437^2 =$	6	$r = 5$
$9053^2 - 67 \cdot 1106^2 =$	-3	$r = 7$
$48842^2 - 67 \cdot 5967^2 =$	1	$r = 8$

(Оригинальное индийское решение этой задачи использует прием, сокращающий вычисления. Обе части формулы  $221^2 - 67 \cdot 27^2 = -2$  возводятся в квадрат, что приводит к равенству  $(221^2 + 67 \cdot 27^2)^2 - 67 (2 \cdot 27 \cdot 221)^2 = (-2)(-2)$ , после сокращения которого на  $2^2$  получается окончательное решение  $48\,842^2 - 67 \cdot 5967^2$ . Заметим, что это есть приведенное выше диофантово решение с  $m = 221$ ,  $n = 27$ ,  $Am^2 - n^2 = 2$ .) Коротко говоря, если  $A = 67$  — данное число, то  $x = 5967$  обладает тем свойством, что  $Ax^2 + 1$  является квадратом. «Бесконечное число» решений, которых требует Ферма, можно получить либо продолжая этот процесс и находя все больше равенств, в которых правая часть равна 1 (и тогда окажется, что числа в правой части будут циклически повторяться: 1, -3, 6, -7, -2, -7, 6, -3, 1, -3, 6, — возможно поэтому такой процесс называется «циклическим методом»), либо используя уже найденное решение и получая другие возведением в квадрат:

$$\begin{aligned} 1 &= (48842^2 - 67 \cdot 5967^2)^2 = \\ &= (48842^2 + 67 \cdot 5967^2)^2 - 67(2 \cdot 5967 \cdot 48842)^2 \end{aligned}$$

в куб

$$\begin{aligned}
 1 &= [(48842^2 + 67 \cdot 5967^2)^2 - 67(2 \cdot 5967 \cdot 48842)^2](48842^2 - 67 \cdot 5967^2) = \\
 &= [48842(48842^2 + 67 \cdot 5967^2) + 67 \cdot 2 \cdot 48842 \cdot 5967^2]^2 - \\
 &\quad - 67[5967(48842^2 + 67 \cdot 5967^2) + 48842^2 \cdot 2 \cdot 5967]^2 = \\
 &= (48842^3 + 3 \cdot 67 \cdot 48842 \cdot 5967^2)^2 - 67(3 \cdot 48842^2 \cdot 5967 + 67 \cdot 5967^3)^2,
 \end{aligned}$$

в четвертую степень, и т. д. Это решает задачу Ферма в частном случае  $A = 67$ .

Точно так же можно применять циклический метод для нахождения решения задачи Ферма при произвольном  $A$ , которое не является квадратом. Коротко говоря, процедура заключается в следующем. На первом шаге берем равенство  $1^2 - A \cdot 0^2 = 1$ . Предположим, что на  $n$ -м шаге мы имеем равенство  $p^2 - Aq^2 = k$ . Для того чтобы перейти к  $(n + 1)$ -му шагу, умножим это равенство на  $r^2 - A = s$ ; получим  $(pr + qA)^2 - A(p + qr)^2 = ks$ , где  $r$ , а тем самым и  $s$  еще должны быть определены. В качестве  $r$  выберем положительное целое, для которого  $p + qr$  делится на  $k$  и которому соответствует наименьшее возможное  $s$ . Тогда  $pr + qA$  делится<sup>1)</sup> на  $k$ , и, сократив обе части  $(pr + qA)^2 - A(p + qr)^2 = ks$  на  $k^2$ , мы получим равенство следующего шага  $P^2 - AQ^2 = K$ , где  $P = (pr + qA)/|k|$ ,  $Q = (p + qr)/|k|$  и  $K = s/k$ . Этот процесс продолжается до тех пор, пока на некотором шаге мы не придем к равенству требуемого вида  $p^2 - Aq^2 = 1$ . Тогда  $x = q$  является решением задачи Ферма, так как  $Aq^2 + 1 = p^2$  — квадрат. Затем можно получить бесконечную серию решений, либо продолжая работать циклическим методом для нахождения других равенств  $p^2 - Aq^2 = k$  с  $k = 1$ , либо, как и выше, последовательно возводя в степени первое полученное решение.

В действительности этим методом удастся получить решения задачи Ферма для всех значений  $A$ , которые не являются квадратами. В табл. 1.7 приведен список наименьших решений  $x$  уравнения  $Ax^2 + 1 = \text{квадрат}$  для  $A = 2, 3, 5, 6, \dots$ . Эта таблица показывает, что предложенные Ферма частные случаи  $A = 149$ ,  $A = 109$  являются чрезвычайно трудными. Случай  $A = 61$  — несомненно, труднейший при всех  $A < 100$ , — был также выде-

<sup>1)</sup> Ясно, что  $k$  делит  $(pr + qA)^2$ . Для большинства значений  $k$  отсюда следует, что  $k$  делит  $pr + qA$ , а именно для всех значений  $k$ , которые не делятся на квадраты простых чисел. Здесь же утверждается, что при использовании циклического метода  $k$  всегда делит  $pr + qA$  (даже если получаются значения  $k$ , которые делятся на квадраты простых). Это, как и тот факт, что всегда можно достичь шага, когда  $k = 1$ , и надо доказать, если мы хотим обосновать циклический метод.



Таблица 1.7. Наименьшие решения  $x$  уравнения  $Ax^2+1 = \text{квадрат}$

$A$	$x$	$A$	$x$	$A$	$x$
1	—	51	7	101	20
2	2	52	90	102	10
3	1	53	9100	103	22419
4	—	54	66	104	5
5	4	55	12	105	4
6	2	56	2	106	3115890
7	3	57	20	107	93
8	1	58	2574	108	130
9	—	59	69	109	15140424455100
10	6	60	4	110	2
11	3	61	226153980	111	28
12	2	62	8	112	12
13	180	63	1	113	113296
14	4	64	—	114	96
15	1	65	16	115	105
16	—	66	8	116	910
17	8	67	5967	117	60
18	4	68	4	118	28254
19	39	69	936	119	11
20	2	70	30	120	1
21	12	71	413	121	—
22	42	72	2	122	22
23	5	73	267000	123	11
24	1	74	430	124	414960
25	—	75	3	125	83204
26	10	76	6630	126	40
27	5	77	40	127	419775
28	24	78	6	128	51
29	1820	79	9	129	1484
30	2	80	1	130	570
31	273	81	—	131	927
32	3	82	18	132	2
33	4	83	9	133	224460
34	6	84	6	134	12606
35	1	85	30996	135	21
36	—	86	1122	136	3
37	12	87	3	137	519712
38	6	88	21	138	4
39	4	89	53000	139	6578829
40	3	90	2	140	6
41	320	91	165	141	8
42	2	92	120	142	12
43	531	93	1260	143	1
44	30	94	221064	144	—
45	24	95	4	145	24
46	3588	96	5	146	12
47	7	97	6377352	147	8
48	1	98	10	148	6
49	—	99	1	149	2113761020
50	14	100	—	150	4

лен <sup>1)</sup> Ферма, когда он предложил эту задачу Френиклю примерно в то же самое время. Если и могли быть какие-то сомнения, то этот факт достоверно показывает, что Ферма владел процедурой решения, которая позволяла ему находить самые трудные случаи. (Хотя случай  $A = 433$  не кажется особенно трудным: решение имеет 19 разрядов, а при  $A = 421$  разрядов 33.)

К чести англичан, надо сказать, что им удалось не только найти частные решения в предложенных Ферма трех случаях, но и разработать общую процедуру получения решений для любого значения  $A$ . Кто сделал это — достоверно неизвестно. Хотя Джон Валлис первым дал описание процедуры и получил решения в трех частных случаях, он приписывает авторство виконту Уильяму Броункеру. В опубликованной переписке Валлиса нет никаких указаний на то, что Броункер когда-либо сообщал ему что-либо об этом методе, кроме нескольких простых замечаний, которые, быть может, послужили зародышем идеи, развитой впоследствии Валлисом. Вполне возможно, Валлису было чрезвычайно важно завоевать расположение Броункера и добиться его покровительства, и потому он назвал этот метод методом Броункера; Броункер не только принадлежал к знати, он был также первым президентом Королевского общества <sup>2)</sup>).

Концепция английского метода существенно отличается от концепции описанного выше «циклического метода», хотя вычисления очень похожи. В частности, оба метода обладают тем свойством, что их можно применять для нахождения решений в частных случаях, не будучи заранее уверенным, что это приведет к успеху. Например, выше нам удалось найти решение в случае  $A = 67$ , когда мы получили равенство с правой частью 1; аналогично будет установлено, что при применении циклического метода к любому другому частному случаю мы получим в конце концов равенство с правой частью 1 и тем самым найдем решение поставленной задачи. Однако нет никаких очевидных причин, по которым равенство с правой частью 1 должно обязательно получаться во всех случаях; аналогично, нет очевидных причин, по которым всегда должен приводить к успеху английский метод.

---

<sup>1)</sup> Бхаскара Акхария также выделил случай  $A = 61$  и привел правильное решение  $x = 226\ 153\ 980$  за пять веков до Ферма.

<sup>2)</sup> По крайней мере двое видных ученых сказали мне, что они не согласны с этим мнением — один по той причине, что есть веские основания считать лорда Броункера весьма способным математиком, другой — основываясь на оценке личных качеств Валлиса, который скорее мог приписать себе чужие заслуги, чем отказаться от своих заслуг в пользу другого. Некоторая поддержка моей точки зрения имеется в классическом труде Смита [S3, § 96, стр. 193], где говорится, что Валлис изложил этот метод, «приписывая его лорду Броункеру, хотя, кажется, и ему самому принадлежит некоторая доля в этом изобретении».

Таким образом, англичане в действительности не решили задачу Ферма, которая заключалась в том, чтобы доказать, что «при данном  $A$ , отличном от квадрата, существует бесконечно много таких  $x$ , что  $Ax^2 + 1$  является квадратом», — несмотря на то, что им удалось дать процедуру нахождения  $x$  при данном  $A$ . Конечно, недостает доказательства того, что эта процедура всегда ведет к успеху. Англичане не дали такого доказательства и, кажется, даже не осознавали, что оно необходимо. Однако это обстоятельство далеко не второстепенное, поскольку даже Эйлеру не удалось доказать, что английский метод всегда приводит к успеху. Лишь через 110 лет после того, как Валлис послал ответ на вызов Ферма, Лагранж дал первое доказательство этого утверждения. Доказательство Лагранжа в общих чертах намечено в упражнениях, которые следуют за этим параграфом.

Не вполне ясно, знал ли Ферма об этом недостатке решения Валлиса, и еще менее очевидно, что его собственный метод был свободен от подобного недостатка. Ферма написал письмо, в котором признал, что англичанам в конце концов удалось решить его задачу; в нем он не проявил ни малейшей неудовлетворенности их методом, несмотря на отсутствие доказательства того, что этот метод всегда приводит к решению. Однако главным для Ферма в этом письме было убедить англичан признать, что перед ними была поставлена интересная и достойная их внимания задача. Короче говоря, Ферма по-прежнему надеялся пробудить в Валлисе и его окружении интерес к изучению целых чисел и, быть может, намеренно не обратил внимания на их упущения, чтобы воодушевить их на дальнейшие исследования.

Несколько лет спустя, подводя в письме к Каркави итоги некоторым своим открытиям в теории чисел, Ферма указал, что англичане получили решение его задачи  $Ax^2 + 1 = \text{квадрат}$  только в отдельных частных случаях и что им не удалось дать «общее доказательство». Очевидная интерпретация этого замечания заключается в том, что Ферма заметил отсутствие доказательства того, что предложенный ими процесс всегда приводит к решению; с другой стороны, в нем можно видеть и менее глубокую критику того, что этот процесс описан в недостаточно общих терминах. Ферма утверждает, что он мог бы дать нужное здесь «общее доказательство», «надлежащим образом» применяя метод бесконечного спуска. Трудно понять, как можно использовать бесконечный спуск для доказательства того, что этот процесс — либо метод Валлиса, либо тесно связанный с ним индийский циклический метод — всегда приводит к решению. По этой причине утверждение Ферма нельзя считать несомненным свидетельством в пользу того, что он действительно имел совершенно удовлетворительное решение своей задачи.

В результате ошибки Эйлера эта задача Ферма известна теперь как «уравнение Пелля». Почему-то — возможно, по причине смутных воспоминаний, оставшихся от чтения «Алгебры» Валлиса, — у Эйлера сложилось ошибочное впечатление, будто Валлис приписывает метод решения этой задачи не Броункеру, а Пеллю — современнику Валлиса, который часто упоминается в его работах, но, как оказалось, не имеет ничего общего с решением задачи Ферма. Эйлер впервые сделал эту ошибку еще в 1730 г., когда ему было только 23 года, но она попала и в окончательное издание его «Введения в алгебру» [Е9], написанного около 1770 г. Эйлер был самым популярным математическим автором своего времени, и с тех пор метод Валлиса — Броункера связан с именем Пелля, а задача, которая решается при помощи этого метода, т. е. задача нахождения всех целых решений уравнения  $y^2 - Ax^2 = 1$  с данным числом  $A$ , отличным от квадрата, известна как «уравнение Пелля», несмотря на то, что именно Ферма первым указал на важность этой задачи, а Пелль вообще не имел к ней никакого отношения.

## Упражнения

1. Используя циклический метод, получите несколько значений из табл. 1.7.

2. Английский метод, т. е. метод Валлиса и Броункера, отличается от циклического метода главным образом тем, что вместо выбора  $r^2 - A$  возможно меньшим по абсолютной величине, в нем  $r^2 - A$  выбирается отрицательным, а  $r$  — удовлетворяющим условию  $r^2 < A$  и возможно бóльшим. Поэтому в правой части равенств происходит чередование знаков. Используя этот метод, найдите решения для  $A = 13$  и  $A = 67$  и сравните полученные равенства с теми, которые получаются при циклическом методе. (Для  $A = 13$  правые части равны 1, —4, 3, —3, 4, —1, 4, —3, 3, —4, 1, а для  $A = 67$ : 1, —3, 6, —7, . . .)

3. Докажите, что если  $p^2 - Aq^2 = k$  и  $P^2 - AQ^2 = K$  — две последовательные строчки в процессе циклического или английского метода, то  $r$  исчезает из  $pQ - Pq$  и при этом получается  $pQ - Pq = \pm 1$ . Заключите отсюда, что  $P$  и  $Q$  взаимно просты. Затем получите, что взаимно просты  $Q$  и  $K$ , так что сравнение « $QR + P$  делится на  $K$ », которое определяет следующее значение  $r$ , имеет решения. Наконец, докажите, что любое решение  $R$  этого уравнения удовлетворяет также и сравнению « $QA + PR$  делится на  $K$ », вследствие чего можно выполнить следующий шаг циклического метода.

4. Докажите, что если  $r$  и  $R$  — значения  $r$ , которые соответственно предшествуют и следуют за строчкой  $P^2 - AQ^2 = K$ , то  $r + R$  делится на  $K$ . [ $P - rQ$  делится на  $K$ .] Обратите внимание на то, что это значительно упрощает нахождение  $R$  на каждом шаге.

5. Обратите внимание на то, что указанное в упр. 4 упрощение позволяет вычислять последовательность  $k$  и  $r$ , не прибегая к вычислению  $p$  или  $q$ . Например, докажите, что циклический метод с первыми строчками  $1^2 - 149 \cdot 0^2 = 1$  и  $12^2 - 149 \cdot 1 = -5$  даст решение  $p^2 - 149q^2 = 1$  в предложенном Ферма случае  $A = 149$  в 15-й строчке. (Не надо вычислять решение.) Докажите, что английский метод приведет к решению на 19-м шаге.

6. Докажите, что если  $r$  и  $k$  известны, то вычисление  $p$  и  $q$  можно упростить следующим образом. Пусть  $p^2 - Aq^2 = k$ ,  $P^2 - AQ^2 = K$ ,  $\mathcal{P}^2 - A\mathcal{Q}^2 =$

$= \mathcal{K}$  — три последовательные строчки, и пусть  $r$  и  $R$  — промежуточные значения  $r$ . Тогда

$$\mathcal{P} = nP \pm p, \quad \mathcal{Q} = nQ \pm q,$$

где в качестве знаков надо взять два плюса, если  $Kk < 0$ , и два минуса, если  $Kk > 0$ , и где  $n$  — такое целое, что  $r \mp R = n |K|$ . Используя умножение матриц, эти формулы можно записать в виде

$$\begin{bmatrix} \mathcal{P} & P \\ \mathcal{Q} & Q \end{bmatrix} = \begin{bmatrix} P & p \\ Q & q \end{bmatrix} \begin{bmatrix} n & 1 \\ \pm 1 & 0 \end{bmatrix},$$

Поскольку первые две строчки в таблице найти легко, это дает нам средство для вычисления  $p$  и  $q$ . Например,  $p$  и  $q$  в девятой строчке вычислений для  $A = 67$  являются элементами первого столбца матрицы

$$\begin{bmatrix} 8 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 5 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 9 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 5 & 1 \\ 1 & 0 \end{bmatrix}$$

что значительно упрощает дело. Используя  $r$  и  $k$ , найденные в упр. 5, запишите находящееся в 15-й строчке циклического метода решение уравнения  $p^2 - 149q^2 = 1$  как первый столбец произведения 14 матриц. Перемножьте матрицы и найдите решение  $x = 2\ 113\ 761\ 020$  уравнения Пелля при  $A = 149$ .

7. Докажите, что если два последовательных значения  $k$  одинаковы по абсолютной величине:  $K = \pm k$ , то  $pP \mp AqQ$  и  $pQ \mp qP$  делятся на  $k$ . [Используйте формулу для  $P - rQ$ .] Отсюда следует, что такие две строчки в таблице можно перемножить и результат сократить на  $k^2$ ; при этом получится решение уравнения  $x^2 - Ay^2 = \pm 1$ . В случае  $A = 149$  4-ю и 5-ю строчки можно использовать таким образом для нахождения 8-й строчки. Последнюю можно затем возвести в квадрат и получить 15-ю. Проведите эти вычисления.

8. Найдите решение  $x = 151\ 404\ 244\ 455\ 100$  в случае  $A = 109$  Ферма и Бхаскары.

Оставшиеся упражнения посвящены доказательству того, что циклический метод должен привести к решению уравнения Пелля и что таким способом получаются все решения уравнения Пелля.

9. Английский метод (см. упр. 2) менее эффективен, чем циклический, но он проще в том отношении, что знаки изменяются в нем правильным образом (в упр. 6 всегда появляется знак плюс). Следовательно, доказать, что английский метод всегда дает решение уравнения Пелля и что таким методом могут быть получены все решения, легче, чем доказать то же утверждение о циклическом методе. Докажите, что если строчка  $p^2 - Aq^2 = k$  встречается как в английском, так и в циклическом методе, и если следующие за ней строчки различны, например  $P^2 - AQ^2 = K$  в английском методе и  $\mathcal{P}^2 - A\mathcal{Q}^2 = \mathcal{K}$  в циклическом методе, то  $K \neq 1$  и за строчкой  $P^2 - AQ^2 = K$  в английском методе следует  $\mathcal{P}^2 - A\mathcal{Q}^2 = \mathcal{K}$ . Короче говоря, единственное различие между ними состоит в том, что в циклическом методе могут пропускаться некоторые строчки английского метода, но пропущенные строчки никогда не дают решений уравнения Пелля. Поэтому для того, чтобы доказать, что при циклическом методе получаются все решения уравнения Пелля, достаточно доказать аналогичное утверждение для английского метода. [Пусть  $r$  и  $\mathcal{R}$  — значения  $r$ , которые следуют за строчкой  $p^2 - Aq^2 = k$  в английском и циклическом методах соответственно; предположим, что  $R$  — значение, следующее за  $P^2 - AQ^2 = K$  в английском методе. Поскольку



эти два метода приводят к различным значениям, мы получаем неравенство  $A - r^2 > (r + |k|)^2 - A > 0$ . Из этого неравенства следует, что  $K > -K + 2r - k$  при  $k < 0$  и  $-K > K + 2r + k$  при  $k > 0$ . В первом случае  $(-r + nK)^2 - A$  отрицательно при  $n = 1$  и положительно при  $n = 2$ , следовательно,  $R = -r + K$ . Во втором случае  $R = -r - K$ . Таким образом,  $R = -r + |K|$ . Отсюда получается, что следующее значение  $k$  в английском методе равно  $(R^2 - A)/K = [(r + |k|)^2 - A]/k = \mathcal{K}$ . Аналогично, следующее значение  $q$  в английском методе равно  $|K|^{-1} [P + Q(-r + |K|)] = |k|^{-1} [p + q(r + |k|)] = \mathcal{Q}$ , а следующее значение  $r$  равно  $\mathcal{P}$ . Остается показать, что  $|K| \neq 1$ . Для этого достаточно доказать, что в английском методе всегда выполняется неравенство  $r > 0$ , — это утверждение будет доказано в следующем упражнении. Заметим, что в случае неоднозначной возможности выбора  $(A - r^2 = (r + |k|)^2 - A)$  здесь предполагалось, что циклический метод согласуется с английским, т. е. выбирается меньшее из двух возможных значений  $r$ . Приведенное выше доказательство в действительности показывает, что при выборе большего значения была бы пропущена строчка с  $K \neq 1$ .]

10. Правильное описание английского метода в действительности требует доказательства существования таких значений  $r$ , удовлетворяющих сравнению « $qr + p$  делится на  $k$ », для которых  $r^2 - A < 0$ . Конечно, это зависит от того обстоятельства, что большие значения  $k$  не возникают. На практике обнаруживается, что такие значения  $r$  всегда существуют и положительны. Кроме того, оказывается, что циклы практически встречающихся значений  $k$  и  $r$  являются палиндромами, т. е. не изменяются, если записать их в обратном порядке. Далее, если  $k$  положительно, то  $(r + k)^2 - A > 0$  и, следовательно,  $k + 2r + K$  положительно; если же  $k$  отрицательно, то  $(r - k)^2 - A > 0$  и  $k - 2r + K$  отрицательно. Так как циклы значений  $k$  и  $r$  являются палиндромами, то существует симметрия между значениями  $k$  и  $K$ ; поэтому естественно ожидать, что в каждом множестве из двух последовательных значений  $k$  с промежуточным значением  $r$ , скажем  $k, r, K$ , выполняются неравенства  $k + 2r + K > 0$ ,  $k - 2r + K < 0$ . Отсюда следует, что  $r > 0$ . Докажите эти неравенства; во-первых, докажите, что они выполняются на первом шаге при  $k = 1$ ,  $r = [\sqrt{A}] =$  наибольшее целое меньшее, чем  $\sqrt{A}$ , и  $K = [\sqrt{A}]^2 - A$ , а во-вторых, докажите, что эти неравенства выполняются на любом данном шаге при условии, что они справедливы на предыдущем шаге.

11. Упражнение 10 показывает, что английский метод определяет бесконечную последовательность  $k$ . Предположим, что  $k, K, \mathcal{K}$  — три последовательных значения  $k$ ; допустим также, что  $K$  и  $\mathcal{K}$  позже снова встречаются как последовательные значения в последовательности всех  $k$ . Докажите, что тогда  $k$  вновь предшествует  $K$  и  $\mathcal{K}$ . Покажите, что существует только конечное число возможных значений  $k$ . Заключите отсюда, что английский метод всегда дает некоторое решение уравнения Пелля. [Как указано в упр. 10, циклы значений  $k$  и  $r$  образуют палиндромы; поэтому естественно ожидать, что если  $k, K, \mathcal{K}$  — последовательные значения  $k$ , а  $r, R$  — промежуточные значения  $r$ , то  $r, k$  можно найти по  $\mathcal{K}, R, K$  точно так же, как  $R, \mathcal{K}$  находятся по  $k, r, K$ .]

12. Докажите, что циклы значений  $k$  и  $r$ , полученные английским методом, всегда образуют палиндромы и всегда содержат четное число шагов.

13. Докажите, что английский метод дает все решения уравнения Пелля. [Можно поступить следующим образом. Пусть  $x^2 - Ay^2 = 1$ . Не ограничивая общности, можно считать, что  $x$  и  $y$  положительны. Пусть  $x = x_0, y = y_0$ ; применив английский метод к  $x_0^2 - Ay_0^2 = 1$ , найдите  $x_1^2 - Ay_1^2 = k_1, x_2^2 - Ay_2^2 = k_2, \dots$ . Тогда, согласно упр. 6,  $x_{i+1} = n_i x_i + x_{i-1}, y_{i+1} = n_i y_i + y_{i-1}$ , причем последовательности положительных целых  $n_1, n_2, n_3, \dots$  периодичны. По периодичности последовательность  $n_i$  можно продолжить на все целые  $i$  (не только положительные). Тогда  $x_i, y_i$  можно определить



для всех целых  $i$ . Докажите, что  $x_i^2 - Ay_i^2 = k_i$ ; здесь  $k_i$  определены при отрицательных  $i$  по периодичности. Очевидно, что если  $x_i$  и  $y_i$  положительны при всех  $i \geq j$  (такими они являются при  $j = 0$ ), то  $|x_{j+2}| > |x_j|$ . Согласно принципу бесконечного спуска, должно существовать такое значение  $j$ , что  $x_i$  и  $y_i$  положительны при  $i > j$ , но не обладают этим свойством при  $i = j$ . Рассмотрим матричное уравнение

$$\begin{bmatrix} x_1 & x_0 \\ y_1 & y_0 \end{bmatrix} = \begin{bmatrix} n_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} n_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} n_{j+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_{j+1} & x_j \\ y_{j+1} & y_j \end{bmatrix}.$$

Так как  $x_{j+1}y_j - y_{j+1}x_j = \pm 1$  и  $x_{j+1}, y_{j+1}$  положительны, то  $x_j$  и  $y_j$  не могут иметь противоположные знаки. Но  $x_j^2 - Ay_j^2 = k_j$  и  $|k_j| < A$ , поэтому  $x_j \neq 0$ . Следовательно,  $y_j = 0$ . Тогда  $x_j = \pm 1$  и  $k_j = 1$ . Пусть

$$\begin{bmatrix} P & p \\ Q & q \end{bmatrix} = \begin{bmatrix} n_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} n_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} n_{j+1} & 1 \\ 1 & 0 \end{bmatrix}.$$

Тогда  $x_0 = x_j P$ , так что  $x_j = 1$ . Следовательно,  $x_0 = P$  и  $y_0 = Q$ . Надо только доказать, что английский метод дает решение  $P^2 - AQ^2 = 1$  уравнения Пелля, а это ясно из упр. 6.]

## 1.10. Другие открытия Ферма в теории чисел

Многочисленные недоказанные утверждения Ферма остались вызовом для тех, кто пришел ему на смену, и хотя ему не удалось пробудить интерес к теории чисел ни у Валлиса, ни у других математиков следующего поколения, на более поздних математиков, особенно начиная с Эйлера, попытки доказать или опровергнуть эти утверждения оказали огромное стимулирующее влияние. Как впоследствии выяснилось, все они, за исключением утверждения о том, что числа  $2^{32} + 1, 2^{64} + 1, 2^{128} + 1, \dots$  являются простыми, и, возможно, Последней теоремы  $x^n + y^n \neq z^n$  ( $n > 2$ ), справедливы. Эти утверждения (кроме тех, которые обсуждались выше) не оказали непосредственного влияния на дальнейшую историю Последней теоремы Ферма, поэтому мы не будем рассматривать их подробно. Однако некоторые из них стоит упомянуть хотя бы для того, чтобы дать представление о размахе деятельности Ферма.

Одно из этих утверждений, согласно которому *каждое число можно представить в виде суммы четырех квадратов*, неявно содержится в книге Диофанта и явно сформулировано в комментариях Баше. Ферма утверждал, что он может доказать не только это утверждение, но и его обобщение, согласно которому *каждое число можно представить в виде суммы трех треугольных чисел, или четырех квадратных чисел, или пяти пятиугольных, или шести шестиугольных чисел*, и т. д. — ad infinitum. Здесь треугольными числами называются  $0, 0 + 1 = 1, 1 + 2 = 3, 3 + 3 = 6, 6 + 4 = 10, 10 + 5 = 15$  и т. д.; квадратными — числа  $0, 0 + 1 = 1, 1 + 3 = 4, 4 + 5 = 9, 9 + 7 = 16, 16 + 9 = 25, \dots$ , а пятиугольными — числа  $0, 0 + 1 = 1, 1 + 4 = 5, 5 + 7 = 12, 12 + 10 = 22, 22 + 13 = 35$  и т. д. Вообще,  $n$ -угольные числа  $0,$

$1, a_2, a_3, a_4, \dots$  получаются при последовательном сложении членов арифметической прогрессии  $1, n-1, 2n-3, 3n-5, \dots$ . Таким образом,  $a_0 = 0, a_1 = 1, a_2 = n, a_3 = 3n-3, a_4 = 6n-8, a_5 = 10n-15, \dots, a_j = \frac{1}{2}j(j-1)n - j(j-2)$ . (Многоугольные числа рассматривались в различных древних трактатах, включая трактат Диофанта, от которого до наших времен сохранились только фрагменты.) Впоследствии с этой красивой теоремой были связаны некоторые из величайших имен в истории математики: Лагранж первым доказал утверждение о квадратах, Гаусс — для треугольных чисел, а Коши впервые получил доказательство в общем случае.

Среди других недоказанных утверждений Ферма содержится теорема о том, что  $25 + 2 = 27$  является единственным целочисленным решением уравнения  $x^2 + 2 = y^3$ , а  $4 + 4 = 8$  и  $121 + 4 = 125$  — единственные решения уравнения  $x^2 + 4 = y^3$ . Казалось бы, эти простые утверждения возникли из ничего, и не видно никакого естественного пути, на котором можно было бы попытаться их доказать<sup>1)</sup>. Согласно другому утверждению такого типа,  $1 + 1 + 1 + 1 = 4$  и  $1 + 7 + 49 + 343 = 400$  являются единственными решениями уравнения  $1 + x + x^2 + x^3 = y^2$  (упр. 1).

Адресованное Валлису и другим английским математикам предложение решить уравнение Пелля в действительности было вторым вызовом Ферма. Первый вызов был еще труднее и оказался, по-видимому, выше их понимания. Ферма предложил две задачи. (1) Найти куб, который в сумме со всеми его собственными делителями дает квадрат. [Например, сумма числа 343 и всех его собственных делителей ( $343 + 49 + 7 + 1 = 400$ ) является квадратом. Найдите другой куб, обладающий тем же самым свойством.] (2) Найти квадрат, который в сумме со всеми его собственными делителями дает куб. Решение этих задач можно найти в книге Диксона [D2, т. 1, стр. 54—58].

Еще одна задача Ферма, заинтересовавшая Эйлера, состоит в следующем: дано число, которое является суммой двух кубов; запишите его в виде суммы двух кубов другим способом. Здесь кубы предполагаются рациональными, однако можно обычным образом избавиться от знаменателей и свести задачу к нахождению всех целочисленных решений уравнения  $x^3 + y^3 = u^3 + v^3$ . Френикль, перед которым Ферма поставил эту задачу, нашел несколько решений, например  $1729 = 9^3 + 10^3 = 1^3 + 12^3$  и  $40\,033 = 16^3 + 33^3 = 9^3 + 34^3$  (по-видимому, испытанным методом проб и ошибок).

<sup>1)</sup> Еще до Ферма Баше изучал рациональные решения  $x, y$  уравнения  $x^2 + 2 = y^3$  (см. Диксон [D2, т. 2, стр. 533]). Доказательства этих утверждений Ферма можно найти в упражнениях к § 2.5.

В заключение еще одна теорема, которую легко сформулировать, но далеко не легко доказать: *ни одно треугольное число, большее 1, не является четвертой степенью*. Другими словами, при  $x > 2$  уравнение  $\frac{1}{2}x(x-1) = y^4$  не имеет решений в целых числах. Первое доказательство этого факта примерно через сто пятьдесят лет было опубликовано в «Теории чисел» Лежандра.

В письме к Каркави Ферма завершает подведение итогов своим любимым открытиям в теории чисел следующими словами: «Потомки, возможно, будут благодарны мне за то, что я показал, что Древние знали не всё». Какое драматичное свидетельство пропасти во взглядах между временем Ферма и нашим временем! Невозможно представить себе математика двадцатого века, который считал бы, что Древние знали всё. Напротив, в наше время считается (по крайней мере в том, что касается математики), что Древние вообще ничего не знали. Скорее мы можем быть благодарны Ферма за то, что он показал нам, какое стимулирующее влияние оказывает изучение работ великих деятелей науки прошлого и как оно способствует более глубокому проникновению в предмет.

## Упражнение

1. Докажите утверждение Ферма о том, что единственными натуральными числами  $x$ , для которых  $1 + x + x^2 + x^3$  — квадрат, являются  $x = 1$  и  $x = 7$ . Кроме них единственными целыми решениями являются  $x = 0$ ,  $-1$ . [Это прекрасная, но очень трудная задача. Воспользуйтесь тем, что  $x^4 + y^4$  не может быть квадратом (§ 1.5), а уравнение  $x^4 - y^4 = z^2$  разрешимо только в тривиальных случаях  $y = 0$  или  $z = 0$  (§ 1.6, упр. 2).]

## Глава 2

### ЭЙЛЕР

#### 2.1. Эйлер и Последняя теорема Ферма при $n = 3$

Леонард Эйлер (1707—1783), несомненно, был величайшим математиком своего времени. Он внес вклад во все мыслимые области математики — от прикладной математики до алгебраической топологии и теории чисел, причем не только в виде новых теорем и методов, но и в виде целой серии учебников по алгебре, анализу, математической физике и другим областям. Эти учебники составили основу математического образования для нескольких последующих поколений.

О величии Эйлера как математика можно судить хотя бы по тому, что при изучении теории чисел создается впечатление, что Эйлер в основном интересовался теорией чисел; если же изучаешь расходящиеся ряды или дифференциальные уравнения, то кажется, что именно расходящиеся ряды или дифференциальные уравнения были для Эйлера любимым предметом исследования и т. д. Конечно, в этой книге мы будем главным образом интересоваться вкладом Эйлера в теорию чисел и, в частности, его достижениями, связанными с Последней теоремой Ферма. Независимо от того, была или не была теория чисел любимым предметом Эйлера, в течение всей своей жизни он проявлял к ней неослабевающий интерес, и одних только его результатов в этой области было бы достаточно, чтобы его имя навсегда осталось в анналах математики.

В истории Последней теоремы Ферма имеются противоречивые мнения о том, удалось ли Эйлеру доказать эту теорему при  $n = 3$ . Обычно считается, что Эйлер привел доказательство случая  $n = 3$ , но оно было «неполным» в некотором важном отношении. В нескольких словах невозможно сформулировать суть дела точнее. Подробное объяснение значительно сложнее. Доказательство Эйлера содержало фундаментальный пробел, о котором Эйлер, очевидно, не подозревал. Исправить это доказательство непосредственно, т. е. предложить другое доказательство того утверждения, при доказательстве которого Эйлер допустил ошибку, далеко не просто. Однако, как мы покажем в § 2.5, это доказательство можно исправить косвенным образом — при помощи рассуждений, которые Эйлер применил при доказательстве других утверждений Ферма. Такой метод не дает ответа на вопрос о том, можно ли залатать первоначальное доказательство Эйлера — что весьма жела-

тельно ввиду элегантности и общности этого доказательства — но он по крайней мере показывает, что уравнение  $x^3 + y^3 = z^3$  неразрешимо в целых положительных числах  $x, y, z$ .

## 2.2. Доказательство Эйлера для $n = 3$

В своем доказательстве Последней теоремы Ферма при  $n = 3$  Эйлер применяет принадлежащий Ферма метод *бесконечного спуска*. Он показывает, что если можно найти положительные целые числа  $x, y, z$ , удовлетворяющие уравнению  $x^3 + y^3 = z^3$ , то существуют меньшие положительные целые с тем же свойством; таким образом, в случае разрешимости этого уравнения можно было бы найти убывающую бесконечную последовательность таких троек целых положительных чисел. Ясно, что такой последовательности не существует. Следовательно, нельзя найти таких чисел  $x, y, z$ .

Итак, предположим, что  $x^3 + y^3 = z^3$ . Из этого уравнения следует, что любой делитель двух из трех чисел  $x, y, z$  делит также и третье из них. Следовательно, обе части этого уравнения можно сократить на все общие делители и с самого начала считать, что числа  $x, y, z$  *попарно взаимно просты*, т. е. что наибольший общий делитель  $x, y$ , или  $x, z$ , или  $y, z$  равен 1. В частности, не более чем одно из чисел  $x, y, z$  может быть четным. В то же время ясно, что по крайней мере одно из этих чисел является четным: если  $x$  и  $y$  оба нечетны, то  $z$  четно. Поэтому в точности одно из этих чисел является четным.

Сначала предположим, что  $x, y$  нечетны, а  $z$  четно. Тогда  $x + y$  и  $x - y$  — четные числа, скажем  $2p$  и  $2q$  соответственно, и  $x = \frac{1}{2}(2p + 2q) = p + q$ ,  $y = \frac{1}{2}(2p - 2q) = p - q$ . Если  $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$  выразить через  $p$  и  $q$ , то получим

$$2p [(p + q)^2 - (p + q)(p - q) + (p - q)^2] = 2p (p^2 + 3q^2).$$

Числа  $p$  и  $q$  имеют противоположную четность (поскольку  $p + q$  и  $p - q$  нечетны) и взаимно просты: действительно, любой общий делитель этих чисел обязан делить  $x = p + q$  и  $y = p - q$  и поэтому должен равняться 1. Кроме того, можно предположить, что  $p$  и  $q$  положительны. (Если  $x < y$ , то, меняя местами  $x$  и  $y$ , можно получить  $q > 0$ . С другой стороны,  $x \neq y$ , поскольку в противном случае  $x = y = 1$ ,  $z^3 = 2$ .) Следовательно, из предположения о существовании нечетных  $x, y$ , удовлетворяющих уравнению  $x^3 + y^3 = z^3$ , следует, что существуют такие взаимно простые положительные целые  $p$  и  $q$  противоположной четности, что

$$2p (p^2 + 3q^2) = \text{куб целого числа}.$$

К такому же выводу можно прийти при нечетном  $z$  и четном  $x$  или  $y$ . В этом случае нечетное число, скажем  $y^3$ , можно перенести

в правую часть:

$$x^3 = z^3 - y^3 = (z - y)(z^2 + zy + y^2).$$

Тогда  $z - y = 2p$ ,  $z + y = 2q$ ,  $z = q + p$ ,  $y = q - p$  и

$$x^3 = 2p [(q + p)^2 + (q + p)(q - p) + (q - p)^2],$$

что приводит к тому же самому заключению:

$$2p(p^2 + 3q^2) = \text{куб целого числа},$$

где  $p$  и  $q$  — взаимно простые положительные целые противоположной четности.

Следующий шаг в нашем рассуждении, грубо говоря, состоит в том, чтобы заметить, что числа  $2p$  и  $p^2 + 3q^2$  взаимно просты, и из этого замечания заключить, что их произведение может быть кубом тогда и только тогда, когда каждый из сомножителей является кубом. Обратите внимание на аналогию с методом из § 1.3, где анализируются решения уравнения  $x^2 + y^2 = z^2$ . Однако утверждение, что  $2p$  и  $p^2 + 3q^2$  взаимно просты, не вполне обосновано. Так как  $p$  и  $q$  имеют противоположную четность, то  $p^2 + 3q^2$  — нечетное число, и каждый общий делитель чисел  $2p$ ,  $p^2 + 3q^2$  обязан быть общим делителем чисел  $p$ ,  $p^2 + 3q^2$ , а потому и  $p$ ,  $3q^2$ . Но  $p$  и  $q$  взаимно просты, поэтому отсюда следует, что единственным общим делителем может быть число 3. Однако если 3 делит  $p$ , то оно делит и  $p^2 + 3q^2$  и  $2p$ ; поэтому  $2p$  и  $p^2 + 3q^2$  не взаимно просты. Следовательно, доказательство распадается на два случая: в первом случае 3 не делит  $p$ , а потому  $2p$  и  $p^2 + 3q^2$  взаимно просты, а во втором 3 делит  $p$ . Сначала мы рассмотрим первый случай; второй окажется простой модификацией первого.

Итак, предположим, что 3 не делит  $p$ , и, следовательно,  $2p$  и  $p^2 + 3q^2$  являются кубами. Применяя формулу

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$$

из § 1.7, можно найти кубы вида  $p^2 + 3q^2$ :

$$\begin{aligned} (a^2 + 3b^2)^3 &= (a^2 + 3b^2) [(a^2 - 3b^2)^2 + 3(2ab)^2] = \\ &= [a(a^2 - 3b^2) - 3b(2ab)]^2 + 3[a(2ab) + b(a^2 - 3b^2)]^2 = \\ &= (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2. \end{aligned}$$

Таким образом, один из способов нахождения кубов вида  $p^2 + 3q^2$  состоит в том, чтобы выбрать произвольные числа  $a$ ,  $b$  и положить

$$p = a^3 - 9ab^2, \quad q = 3a^2b - 3b^3,$$

так что  $p^2 + 3q^2 = (a^2 + 3b^2)^3$ . Главный пробел, который надо заполнить в доказательстве Эйлера, заключается в доказательстве утверждения, что такой способ дает *все* кубы вида  $p^2 + 3q^2$ , т. е.



если  $p^2 + 3q^2$  является кубом, то существуют такие  $a$  и  $b$ , что  $p$  и  $q$  задаются приведенными выше формулами. Эйлер обосновывает этот вывод при помощи ошибочного рассуждения, изложенного в следующем параграфе, однако он мог бы опираться и на рассуждение из § 2.5, которое, по существу, тоже принадлежит ему самому. В любом случае, считая это утверждение справедливым, оставшуюся часть доказательства провести сравнительно легко.

Выражения для  $p$  и  $q$  можно разложить на множители:

$$p = a(a - 3b)(a + 3b), \quad q = 3b(a - b)(a + b).$$

Числа  $a$  и  $b$ , конечно, взаимно просты, ибо каждый их общий делитель обязан делить  $p$  и  $q$ , а потому равен 1. Кроме того,

$$2p = 2a(a - 3b)(a + 3b) = \text{куб целого числа.}$$

Числа  $a$  и  $b$  имеют противоположную четность, поскольку в противном случае  $p$  и  $q$  оба были бы четными. Следовательно,  $a - 3b$ ,  $a + 3b$  — нечетные числа, и все возможные общие делители чисел  $2a$ ,  $a \pm 3b$  обязаны делить  $a$ ,  $a \pm 3b$ , а потому и  $a$ ,  $\pm 3b$ . Аналогично, каждый общий делитель чисел  $a + 3b$ ,  $a - 3b$  обязан делить  $a$  и  $3b$ . Короче говоря, единственным возможным общим делителем является число 3. Но 3 не делит  $a$ , поскольку в противном случае оно делило бы  $p$ , что противоречит предположению. Следовательно,  $2a$ ,  $a - 3b$ ,  $a + 3b$  взаимно просты, и каждое из этих чисел должно быть кубом, скажем  $2a = \alpha^3$ ,  $a - 3b = \beta^3$ ,  $a + 3b = \gamma^3$ . Тогда  $\beta^3 + \gamma^3 = 2a = \alpha^3$ , и это дает решение уравнения  $x^3 + y^3 = z^3$ , состоящее из меньших чисел, чем исходное решение.

Точнее,  $\alpha^3\beta^3\gamma^3 = 2a(a - 3b)(a + 3b) = 2p$ . Число  $2p$  положительно и делит  $z^3$ , если  $z$  четно, или  $x^3$ , если  $x$  четно. Тогда в любом случае  $\alpha^3\beta^3\gamma^3$  меньше  $z^3$ . Числа  $\alpha$ ,  $\beta$  и  $\gamma$  не обязаны быть положительными, но  $(-\alpha)^3 = -\alpha^3$ , поэтому отрицательные кубы можно перенести в другую часть уравнения, и мы получим уравнение вида  $X^3 + Y^3 = Z^3$ , где  $X$ ,  $Y$ ,  $Z$  положительны и  $Z^3 < z^3$ . Итак, в случае когда 3 не делит  $p$ , спуск произведен.

Наконец, рассмотрим случай, когда  $3 \mid p$ . Тогда  $p = 3s$  и 3 не делит  $q$ . В этом случае  $2p(p^2 + 3q^2) = 3^2 \cdot 2s(3s^2 + q^2)$ . Легко видеть, что числа  $3^2 \cdot 2s$  и  $3s^2 + q^2$  взаимно просты; следовательно, каждое из них является кубом. Согласно лемме, которую мы докажем позже,  $3s^2 + q^2$  может быть кубом только тогда, когда

$$q = a(a - 3b)(a + 3b), \quad s = 3b(a - b)(a + b)$$

при некоторых целых  $a$  и  $b$ . Число  $3^2 \cdot 2s$  является кубом, поэтому кубом будет  $3^2 \cdot 2b(a - b)(a + b)$ , а следовательно, и  $2b(a - b) \times (a + b)$ . Легко видеть, что множители, входящие в последнее выражение, взаимно просты; таким образом,  $2b = \alpha^3$ ,  $a - b = \beta^3$ ,

$a + b = \gamma^3$ ,  $\alpha^3 = 2b = \gamma^3 - \beta^3$ . Как и выше, отсюда можно получить равенство вида  $X^3 + Y^3 = Z^3$ , где  $Z^3 < z^3$ .

Итак, в любом случае из существования куба, представимого в виде суммы двух кубов, следует существование меньшего куба такого же вида, что невозможно. Для завершения доказательства остается только показать, что если существуют взаимно простые целые  $p$  и  $q$ , для которых  $p^2 + 3q^2$  является кубом, то найдутся такие целые  $a$  и  $b$ , что  $p = a^3 - 9ab^2$  и  $q = 3a^2b - 3b^3$ . Доказательство этого утверждения приведено в § 2.5.

### 2.3. Арифметика иррациональных чисел

Метод, который Эйлер использовал при попытке доказать приведенное в § 2.2 утверждение о кубах вида  $p^2 + 3q^2$ , основывается на смелой идее распространения арифметики целых чисел при помощи операций сложения, вычитания и умножения на «числа» вида  $a + b\sqrt{-3}$  с целыми  $a$  и  $b$ . Ясно, как складывать, вычитать и умножать такие числа (особого упоминания заслуживает только правило умножения  $(a + b\sqrt{-3})(c + d\sqrt{-3}) = ac + ad\sqrt{-3} + bc\sqrt{-3} + bd(-3) = (ac - 3bd) + (ad + bc)\sqrt{-3}$ ); в этой арифметике выполняются обычные законы коммутативности, ассоциативности и дистрибутивности и, кроме того,

$$1 \cdot (a + b\sqrt{-3}) = a + b\sqrt{-3}.$$

Говоря языком современной алгебры, «числа»  $a + b\sqrt{-3}$  образуют коммутативное кольцо с единицей.

Идея использования в вычислениях иррациональностей вида  $a + b\sqrt{-3}$  упрощает вывод достаточных условий для того, чтобы число  $p^2 + 3q^2$  было кубом. Вместо применения формулы

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$$

можно рассуждать следующим образом. Разложим  $p^2 + 3q^2$  на множители:  $(p + q\sqrt{-3})(p - q\sqrt{-3})$ . Если один из этих множителей является кубом, скажем  $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$ , то легко проверить, что сопряженный к нему, который получается заменой  $\sqrt{-3}$  на  $-\sqrt{-3}$ , является кубом сопряженного к  $a + b\sqrt{-3}$ , т.е.  $p - q\sqrt{-3} = (a - b\sqrt{-3})^3$ . Следовательно, согласно коммутативности умножения,  $(p + q\sqrt{-3})(p - q\sqrt{-3}) = [(a + b\sqrt{-3})(a - b\sqrt{-3})]^3$ , т.е.  $p^2 + 3q^2 = (a^2 + 3b^2)^3$ . Другими словами, для того чтобы найти куб вида  $p^2 + 3q^2$ , достаточно положить  $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$ . Разложив  $(a + b\sqrt{-3})^3$  по формуле бинома Ньютона:

$$p + q\sqrt{-3} = a^3 + 3a^2b\sqrt{-3} + 3ab^2(-3) + b^3(-3)\sqrt{-3},$$

мы получим, что, для того чтобы записать  $p^2 + 3q^2$  в виде куба некоторого числа, достаточно найти такие числа  $a$  и  $b$ , что  $p = a^3 - 9ab^2$ ,  $q = 3a^2b - 3b^3$ . Это и есть достаточное условие, найденное в предыдущем параграфе.

В этой части своей «Алгебры» [Е9] Эйлер всерьез путает необходимые и достаточные условия; поэтому очень трудно установить, что же он в действительности имел в виду. В примерах Эйлер, кажется, большей частью имеет дело с достаточными условиями: начиная с  $a$  и  $b$ , находит  $p$  и  $q$ . Но иногда он допускает совершенно ошибочные утверждения. Например, Эйлер пишет: «Если число  $x^2 + cy^2$  должно быть кубом, то отсюда, конечно, можно заключить, что каждый из его иррациональных множителей, а именно  $x + y\sqrt{-c}$  и  $x - y\sqrt{-c}$ , обязан быть кубом, поскольку эти множители взаимно просты в том смысле, что  $x$  и  $y$  не имеют общих делителей»; при этом Эйлер не доказывает, что  $x + y\sqrt{-c}$  и  $x - y\sqrt{-c}$  обязаны быть кубами. В заключении к тому же самому параграфу (§ 191 из последней части) Эйлер совершенно недвусмысленно утверждает: «Если  $ax^2 + cy^2$  нельзя разложить на два рациональных множителя, то нет других решений, кроме приведенных здесь», т. е.  $ax^2 + cy^2$  только тогда может быть кубом, когда существуют такие целые  $p$  и  $q$ , что  $x\sqrt{a} + y\sqrt{-c} = (p\sqrt{a} + q\sqrt{-c})^3$ . Единственный намек на доказательство этого утверждения состоит в приведенном выше рассуждении по аналогии, а именно: *если  $AB$  является кубом и  $A$  и  $B$  взаимно просты, то  $A$  и  $B$  должны быть кубами*. Последнее утверждение является теоремой, которую можно доказать <sup>1)</sup> для *целых*  $A$  и  $B$ ; однако если  $A$  и  $B$  являются числами вида  $p + q\sqrt{-3}$  или  $x\sqrt{a} + y\sqrt{-c}$ , то это доказательство непригодно. В частном случае  $a = 1$ ,  $c = 3$  утверждение Эйлера действительно справедливо (хотя доказательство совсем не такое, как для целых чисел), но существуют значения  $a$  и  $c$ , при которых оно неверно.

Эйлер рассматривает задачу « $x^2 + cy^2 = \text{куб}$ » вслед за несколько более полным обсуждением случая « $x^2 + cy^2 = \text{квадрат}$ ». В первом случае он утверждает, что «если произведение двух чисел, например  $pq$ , должно быть квадратом, то либо  $p = r^2$  и  $q = s^2$ , т. е. оба множителя должны быть квадратами, либо  $p = mr^2$  и  $q = ms^2$ , т. е. сомножители являются квадратами, умноженными на одно и то же число». Здесь снова это утверждение справедливо, если под «числами» понимаются «целые числа», и мы доказали его в § 1.4; однако Эйлер сразу же применяет этот принцип к числам, которые не являются обыкновенными целыми числами, а имеют вид  $x + y\sqrt{-c}$ . Обсуждение квадратов является более полным,

<sup>1)</sup> Доказательство аналогичного утверждения для квадратов, приведенное в § 1.4, немедленно обобщается на кубы.

чем обсуждение кубов, в том отношении, что Эйлер приводит нечто похожее на альтернативное доказательство утверждения, согласно которому для любого квадрата вида  $x^2 + cy^2$  с взаимно простыми целыми числами  $x$  и  $y$  при некоторых целых  $a$  и  $b$  справедливо равенство  $x + y\sqrt{-c} = (a + b\sqrt{-c})^2$ . Это «доказательство» следует стандартному методу Диофанта, при котором квадратный корень из  $x^2 + cy^2$  записывается в виде  $x + (p/q)y$  с некоторыми целыми числами  $p$  и  $q$ , а затем производятся следующие упрощения:

$$\left(x + \frac{p}{q}y\right)^2 = x^2 + cy^2,$$

$$\frac{2p}{q}xy + \frac{p^2}{q^2}y^2 = cy^2,$$

$$\frac{2p}{q} \frac{x}{y} = \frac{cq^2 - p^2}{q^2},$$

$$\frac{x}{y} = \frac{cq^2 - p^2}{2pq}.$$

«Но  $x$  и  $y$  должны быть взаимно простыми (так же, как  $p$  и  $q$ ), следовательно,  $x = cq^2 - p^2$  и  $y = 2pq$ », так что<sup>1)</sup>  $x + y\sqrt{-c} = (p + q\sqrt{-c})^2$ . Эйлер утверждает, что этот альтернативный вывод «подтверждает<sup>2)</sup> правильность метода», однако из естественного предположения о взаимной простоте  $p$  и  $q$  не следует взаимная простота  $cq^2 - p^2$  и  $2pq$ , а потому не следует и заключение Эйлера о том, что  $x = cq^2 - p^2$ ,  $y = 2pq$ . На самом деле пример  $49 = 2^2 + 5 \cdot 3^2$  не только показывает неадекватность этого рассуждения, но и говорит о том, что само заключение неверно. Действительно, уравнения  $2 = 5q^2 - p^2$ ,  $3 = 2pq$  не имеют рациональных решений  $p$  и  $q$ , не говоря уже о целых решениях. (Эти гиперболы пересекаются при  $p = \sqrt{5/2}$ ,  $q = \sqrt{9/10}$  и  $p = -\sqrt{5/2}$ ,  $q = -\sqrt{9/10}$ .)

Высказывалось мнение ([D2, т. 2, гл. XX, а также стр. xiv]), что сам Эйлер замечает ошибочность предложенного им метода, когда (в § 195) он говорит, что при решении уравнения  $2x^2 - 5 =$  куб его методом потребовалось бы положить  $x\sqrt{2} + \sqrt{5} = (a\sqrt{2} + b\sqrt{5})^3 = a^3 2\sqrt{2} + 3a^2 b 2\sqrt{5} + 3ab^2 5\sqrt{2} + b^3 5\sqrt{5}$  и, следовательно,  $x = 2a^3 + 15ab^2$ ,  $1 = 6a^2 b + 5b^3$ . Из последнего уравнения следует, что  $b = \pm 1$  и  $6a^2 + 5b^2 = \pm 1$ . Ясно, что это невозможно. Следовательно, этот метод показывает, что  $2x^2 - 5$

<sup>1)</sup> Незначительное несовпадение в знаке можно исправить, положив  $-x = cq^2 - p^2$  и  $-y = 2pq$ , так что  $x + y\sqrt{-c} = (p - q\sqrt{-c})^2$ .

<sup>2)</sup> Обратите внимание на то, что это высказывание явно свидетельствует о неуверенности Эйлера в правильности его метода.

не может быть кубом, несмотря на то что это выражение является кубом при  $x = 4$ . Первоначальная реакция Эйлера на это противоречие заключалась в замечании: «Чрезвычайно важно установить причины этого противоречия». Естественно считать, что в этом замечании Эйлер признает важный недочет своего метода и предлагает изучить его причины. Однако, как ясно показывают следующие два параграфа (§ 196, 197), Эйлер был убежден в том, что источник затруднений заключается в знаке минус в выражении  $2x^2 - 5y^2$  и в связанном с этим обстоятельством наличии решений уравнения Пелля  $x^2 - 10y^2 = 1$ , отличных от тривиального решения  $x = \pm 1, y = 0$  (см. упр. 2). Не вникая в детали, достаточно сказать, что Эйлер, по-видимому, был уверен в том, что подобные трудности не возникнут в тех случаях, когда соответствующее выражение имеет знак плюс. Однако, как было указано выше, его метод не приводит к успеху в случае  $49 = 2^2 + 5 \cdot 3^2$ , а здесь второе слагаемое положительно и соответствующее уравнение  $x^2 + 5y^2 = 1$  имеет только тривиальное решение.

В 1753 г. Эйлер заявил, что он может доказать Последнюю теорему Ферма при  $n = 3$  (письмо от 4 августа 1753 г. к Гольдбаху, приведенное в [F6]); однако единственным опубликованным им доказательством является доказательство из «Алгебры» (1770). Размышляя об этом ошибочном доказательстве, разумно предположить, что в своем первоначальном методе он использовал менее оригинальное рассуждение, показывающее, что  $x^2 + 3y^2 = \text{куб}$  только тогда, когда  $x = a^3 - 9ab^2, y = 3a^2b - 3b^3$ , и что лишь позже ему пришла в голову элегантная — но неверная — идея доказать это утверждение, используя тот «факт», что произведение двух взаимно простых сомножителей  $x + y\sqrt{-3}$  и  $x - y\sqrt{-3}$  является кубом, только если кубами являются оба сомножителя. Независимо от того, правильно или нет это предположение, тех идей, которые Эйлер использовал в более ранней работе, достаточно для доказательства необходимой леммы о кубах вида  $x^2 + 3y^2$ .

## Упражнения

1. «Число»  $x + y\sqrt{-c}$  называется *единицей*, если оно является делителем 1, т. е. если существует другое «число» такого же вида, произведение которого на данное число равно 1. Докажите, что единицы взаимно однозначно соответствуют решениям уравнения  $x^2 + cy^2 = \pm 1$ . Найдите все единицы вида  $x + y\sqrt{2}$ . (Укажите способ нахождения бесконечного числа единиц и попытайтесь найти их все. Не нужно доказывать, что вы нашли все единицы.) Найдите все единицы вида  $x + y\sqrt{-41}$ ; вида  $x + y\sqrt{-7}$ ; вида  $x + y\sqrt{7}$ ; вида  $x + y\sqrt{-1}$ .

2. Предположим, что  $f^2 - 10g^2 = 1$  и  $x\sqrt{2} + y\sqrt{5} = (f + g\sqrt{10}) \times (a\sqrt{2} + b\sqrt{5})^3$ . Докажите, что  $2x^2 - 5y^2$  является кубом, даже если

$x\sqrt{2} + y\sqrt{5}$  не равно кубу вида  $(u\sqrt{2} + v\sqrt{5})^3$ . Эйлер считал, что это явление объясняет, почему его методом не удастся найти решение  $x=4$  уравнения  $2x^2 - 5 = \text{куб}$ . Покажите, что  $4\sqrt{2} + \sqrt{5}$  имеет такой вид при  $a=2$ ,  $b=-1$ .

## 2.4. Эйлер о суммах двух квадратов

В 1747 г. сорокалетнему Эйлеру удалось доказать теорему Ферма о том, что каждое простое число вида  $4n + 1$  является суммой двух квадратов. В письме Гольдбаху от 6 мая 1747 г. [F6], в котором он приводит доказательство этой теоремы, Эйлер говорит, что его основная цель состояла в доказательстве другой теоремы Ферма, согласно которой каждое число можно представить в виде суммы не более четырех квадратов. Однако доказательство последней теоремы ускользало от Эйлера до тех пор, пока ее не доказал Лагранж в 1770 г. (после чего Эйлеру удалось значительно упростить доказательство), а доказанные Эйлером теоремы о суммах двух квадратов представляют значительную ценность. В частности, развитые для их доказательства методы позволили Эйлеру доказать основные факты о числах вида  $x^2 + 3y^2$ , а как будет показано в следующем параграфе, те же методы можно использовать для доказательства утверждений о кубах вида  $x^2 + 3y^2$ , которые требуются при доказательстве Последней теоремы Ферма в случае  $n = 3$ .

Доказательство Эйлера теоремы о том, что каждое простое число вида  $4n + 1$  можно представить в виде суммы двух квадратов, не требует много места и совершенно элементарно. (См. письма к Гольдбаху, а также [E8].)

(1) *Произведение двух чисел, каждое из которых является суммой двух квадратов, представимо в виде суммы двух квадратов.* Это утверждение немедленно следует из формулы

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

(2) *Если число, представимое в виде суммы двух квадратов, делится на простое число, являющееся суммой двух квадратов, то частное также является суммой двух квадратов.* Предположим, например, что  $a^2 + b^2$  делится на простое число вида  $p^2 + q^2$ . Тогда  $p^2 + q^2$  делит  $(pb - aq)(pb + aq) = p^2b^2 - a^2q^2 = p^2b^2 + p^2a^2 - p^2a^2 - a^2q^2 = p^2(a^2 + b^2) - a^2(p^2 + q^2)$ . Поскольку это число простое, оно обязано делить либо  $pb - aq$ , либо  $pb + aq$ . Предположим сначала, что  $p^2 + q^2$  делит  $pb + aq$ . Тогда из тождества  $(a^2 + b^2)(p^2 + q^2) = (ap - bq)^2 + (aq + bp)^2$  следует, что  $p^2 + q^2$  должно делить также и  $(ap - bq)^2$ . Следовательно, обе части этого тождества можно разделить на квадрат числа  $p^2 + q^2$ , и в результате получится требуемое выражение  $(a^2 + b^2)/(p^2 + q^2)$  в виде суммы двух квадратов. Второй случай, когда  $p^2 + q^2$  делит



$pb - aq$ , можно рассмотреть аналогичным образом, используя тождество  $(a^2 + b^2)(q^2 + p^2) = (aq - bp)^2 + (ap + bq)^2$ .

(3) Если число, представимое в виде суммы двух квадратов, делится на число, которое не является суммой двух квадратов, то частное имеет делитель, который не представим в виде суммы двух квадратов. По существу, это противоположное к (2) утверждение. Предположим, что  $x$  делит  $a^2 + b^2$  и что разложение частного на простые множители имеет вид  $p_1 p_2 \dots p_n$ . Тогда  $a^2 + b^2 = x p_1 p_2 \dots p_n$ . Если бы все множители  $p_1, p_2, \dots, p_n$  были представимы в виде суммы двух квадратов, то  $a^2 + b^2$  можно было бы последовательно разделить на  $p_1, p_2, \dots, p_n$ , и из утверждения (2) мы получили бы, что каждое частное, до  $x$  включительно, представимо в виде суммы двух квадратов. Следовательно, если  $x$  не является суммой двух квадратов, то хотя бы один из простых множителей  $p_1, p_2, \dots, p_n$  не представим в виде суммы двух квадратов.

(4) Если  $a$  и  $b$  взаимно просты, то каждый делитель числа  $a^2 + b^2$  является суммой двух квадратов. Пусть  $x$  — делитель  $a^2 + b^2$ . Представим  $a$  и  $b$  в виде  $a = tx \pm c$ ,  $b = nx \pm d$ , где  $c$  и  $d$  не превосходят  $x/2$  по абсолютной величине. Тогда  $a^2 + b^2 = t^2 x^2 \pm 2txc + c^2 + n^2 x^2 \pm 2nxd + d^2 = Ax + (c^2 + d^2)$  делится на  $x$ , поэтому  $c^2 + d^2$  должно делиться на  $x$ , скажем  $c^2 + d^2 = yx$ . Если  $c$  и  $d$  имеют общий делитель, больший единицы, то он не может делить  $x$ , поскольку тогда он делил бы  $a$  и  $b$ , что противоречит предположению. Следовательно, обе части равенства  $c^2 + d^2 = yx$  можно сократить на квадрат наибольшего общего делителя чисел  $c$  и  $d$  и получить равенство вида  $e^2 + f^2 = zx$ . Кроме того,  $z \leq x/2$ , поскольку  $zx = e^2 + f^2 \leq c^2 + d^2 \leq (x/2)^2 + (x/2)^2 = x^2/2$ . Если бы  $x$  не был суммой двух квадратов, то, согласно (3), нашелся бы такой делитель числа  $z$  (обозначим его  $w$ ), который нельзя представить в виде суммы двух квадратов. Но это привело бы к бесконечному спуску — переходу от числа  $x$ , которое не является суммой двух квадратов, но делит сумму квадратов двух взаимно простых чисел, к меньшему числу  $w$ , обладающему такими же свойствами. Следовательно,  $x$  должен быть суммой двух квадратов.

(5) Каждое простое число вида  $4n + 1$  является суммой двух квадратов. Следующее элегантное доказательство этого утверждения Эйлер впервые сообщил Гольдбаху в 1749 г. — предложенное двумя годами раньше первое доказательство в этом месте было довольно неясным. Если  $p = 4n + 1$  — простое число, то, согласно теореме Ферма, каждое из чисел  $1, 2^{4n}, 3^{4n}, \dots, (4n)^{4n}$  на единицу больше некоторого кратного  $p$ . (Следующее за  $(4n)^{4n}$  число  $p^{4n}$  делится на  $p$ , а все последующие числа от  $(p + 1)^{4n}$  до  $(2p - 1)^{4n}$  на единицу больше некоторого кратного  $p$ , и т. д.) Следовательно, все разности  $2^{4n} - 1, 3^{4n} - 2^{4n}, \dots, (4n)^{4n} - (4n - 1)^{4n}$  делятся

на  $p$ . Каждую из этих разностей можно разложить в произведение вида  $a^{4n} - b^{4n} = (a^{2n} + b^{2n})(a^{2n} - b^{2n})$ , и  $p$ , как простое число, обязано делить один из множителей. Если хотя бы в одном из  $4n - 1$  случаев оно делит первый множитель, то, ввиду (4) и взаимной простоты данного числа и следующего за ним,  $p$  является суммой двух квадратов. Поэтому достаточно доказать, что  $p$  не может делить все  $4n - 1$  чисел  $2^{2n} - 1, 3^{2n} - 2^{2n}, \dots, (4n)^{2n} - (4n - 1)^{2n}$ . Это легко сделать следующим образом. Если бы  $p$  делило все эти числа, то оно делило бы и все  $4n - 2$  разности следующих друг за другом чисел, все  $4n - 3$  разности этих разностей, и т. д. Но нетрудно убедиться (см. упр. 2), что  $k$ -е разности последовательности  $1^k, 2^k, 3^k, 4^k, \dots$  постоянны и равны  $k!$  (см. табл. 2.4.1). Таким образом, все  $2n$ -е разности

Таблица 2.4.1. Разности от  $x^k$

$k=1$	1	2	3	4	5	6	7		
1-е разности	1	1	1	1	1	1	...		
2-е разности		0	0	0	0	0	0		
$k=2$	1	4	9	16	25	36	49	...	
1-е разности	3	5	7	9	11	13	...		
2-е разности		2	2	2	2	2	...		
3-и разности			0	0	0	0	...		
$k=3$	1	8	27	64	125	216	343	512	...
1-е разности	7	19	37	61	91	127	169	...	
2-е разности		12	18	24	30	36	42	...	
3-и разности			6	6	6	6	6	...	
4-е разности				0	0	0	0	...	
$k=4$	1	16	81	256	625	1296	2401	4096	...
1-е разности	15	65	175	369	671	1105	1695	...	
2-е разности		50	110	194	302	434	590	...	
3-и разности			60	84	108	132	156	...	
4-е разности				24	24	24	24	...	
5-е разности					0	0	0	...	

последовательности  $1, 2^{2n}, 3^{2n}, 4^{2n}, \dots$  равны  $(2n)!$  и, следовательно, не делятся на  $p = 4n + 1$ . Если бы  $p$  делило первые  $4n - 1$  первых разностей  $2^{2n} - 1, 3^{2n} - 2^{2n}, \dots, (4n)^{2n} - (4n - 1)^{2n}$ , то оно делило бы и первые  $4n - 2n$   $2n$ -х разностей, что не имеет места. Следовательно,  $p$  не делит хотя бы одну из этих  $4n - 1$  первых разностей, что и требовалось показать.

В важном письме 1658 г. к Дигби, опубликованном в собрании работ Валлиса и потому, вероятно, известном Эйлеру, Ферма

[F4] утверждает, что он получил неопровержимые доказательства (firmissimus demonstrationibus) следующих утверждений: (a) каждое простое число вида  $4n + 1$  является суммой двух квадратов; (b) каждое простое вида  $3n + 1$  представимо в виде  $a^2 + 3b^2$ , (c) каждое простое вида  $8n + 1$  или  $8n + 3$  представимо в виде  $a^2 + 2b^2$  и (d) каждое число является суммой трех или меньше треугольных чисел, четырех или меньше квадратов, пяти или меньше пятиугольных чисел, и т. д. Эйлер жаждал доказать последнее из этих утверждений — особенно в той части, где говорится, что каждое число представимо в виде суммы не более четырех квадратов, поэтому для него было естественным попытаться использовать методы, которыми он доказал первое из этих утверждений, для доказательства остальных. Он обнаружил, что (c) и (d) по-прежнему недостижимы для него, однако утверждение (b) можно доказать почти так же, как (a).

Главное различие между доказательствами утверждений (a) и (b) состоит в рассмотрении простого числа 2. Заметим, что для представлений чисел в виде  $a^2 + 3b^2$  утверждение (4) неверно. Действительно,  $1^2 + 3 \cdot 1^2$  делится на 2, но 2 не представимо в виде  $a^2 + 3b^2$ . Заметим также, что если доказательство утверждения (4) применить к представлениям в виде  $a^2 + 3b^2$ , то неравенство  $zx \leq (x/2)^2 + (x/2)^2 = x^2/2$  заменится на  $zx \leq (x/2)^2 + 3(x/2)^2 = x^2$ . Таким образом,  $z \leq x$  и отсутствует строгое неравенство, которое требуется для осуществления спуска. Однако если  $x$  нечетно, то неравенства  $|c| \leq x/2$ ,  $|d| \leq x/2$  превращаются в строгие неравенства  $|c| < x/2$ ,  $|d| < x/2$ , и получается требуемое неравенство  $z < x$ . Доказательство аналога утверждения (4) для представлений в виде  $a^2 + 3b^2$  можно провести следующим образом.

(1') Произведение двух чисел, каждое из которых можно представить в виде  $a^2 + 3b^2$ , само представляется в таком виде. Это утверждение следует из тождества  $(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$ .

(2') Если число вида  $a^2 + 3b^2$  делится на 2, то оно должно делиться на 4, и частное от деления на 4 само должно иметь вид  $c^2 + 3d^2$ . Если  $a$  и  $b$  имеют противоположную четность, то  $a^2 + 3b^2$  не делится на 2. Если  $a$  и  $b$  четны, то  $a^2 + 3b^2$  делится на  $2^2$ , и частное имеет вид  $c^2 + 3d^2$ , где  $c = a/2$ ,  $d = b/2$ . Наконец, рассмотрим случай нечетных  $a$  и  $b$ . Тогда  $a = 4m \pm 1$  и  $b = 4n \pm 1$  при соответствующем выборе чисел  $m$  и  $n$  и знаков. Следовательно, либо  $a + b$ , либо  $a - b$  делится на 4. Если  $a + b$  делится на 4, то  $4(a^2 + 3b^2) = (1^2 + 3 \cdot 1^2)(a^2 + 3b^2) = (a - 3b)^2 + 3(a + b)^2$  делится на  $4^2$ . Действительно,  $a - 3b = (a + b) - 4b$ . Отсюда следует, что  $(a^2 + 3b^2)/4$  имеет вид  $c^2 + 3d^2$ . Если  $a - b$  делится на 4, то к такому же выводу можно прийти, используя представление  $4 = (-1)^2 + 3 \cdot 1^2$  вместо  $4 = 1^2 + 3 \cdot 1^2$ .

(3') Если число вида  $a^2 + 3b^2$  делится на простое вида  $p + 3q^2$ , то частное представимо в виде  $c^2 + 3d^2$ . Основной шаг в доказательстве утверждения снова состоит в замечании, согласно которому  $(pb - aq)(pb + aq) = p^2b^2 + 3q^2b^2 - 3q^2b^2 - a^2q^2 = b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)$  делится на  $p^2 + 3q^2$ . Но  $p^2 + 3q^2$  — простое, следовательно, либо  $pb - aq$ , либо  $pb + aq$  делится на  $p^2 + 3q^2$ . Таким образом, при правильном выборе знака  $(p^2 + 3q^2)(a^2 + 3b^2) = [p^2 + 3(\pm q)^2](a^2 + 3b^2) = (pa \mp 3qb)^2 + 3(pb \pm aq)^2$  можно разделить на  $(p^2 + 3q^2)^2$ ; отсюда следует, что  $(a^2 + 3b^2)/(p^2 + 3q^2)$  имеет требуемый вид.

(4') Если число, которое можно записать в виде  $a^2 + 3b^2$ , имеет нечетный делитель, не представимый в таком виде, то и частное имеет нечетный делитель, который не представим в таком виде. Пусть  $xy = a^2 + 3b^2$ , где  $x$  нечетно. Если  $y$  четно, то, согласно (2'), оно делится на 4 и  $x(y/4) = c^2 + 3d^2$ . Этот процесс можно продолжать до тех пор, пока  $y/4^k$  не станет нечетным. Следовательно,  $y = p_1 p_2 \dots p_n$ , где каждое из чисел  $p_1, \dots, p_n$  либо равно 4, либо является нечетным простым. Если все нечетные простые, входящие в это разложение числа  $y$ , можно записать в виде  $c^2 + 3d^2$ , то  $xy = a^2 + 3b^2$  можно последовательно разделить на каждое из чисел  $p_1, \dots, p_n$  и из утверждений (2') и (3') мы получим, что  $x$  можно представить в виде  $c^2 + 3d^2$ . Следовательно, если  $x$  непредставимо в таком виде, то  $y$  должно иметь нечетный делитель, который также нельзя представить в виде  $c^2 + 3d^2$ .

(5') Если  $a$  и  $b$  взаимно просты, то каждый нечетный делитель числа  $a^2 + 3b^2$  представим в виде  $c^2 + 3d^2$ . Пусть  $x$  — нечетный делитель числа  $a^2 + 3b^2$ . Тогда  $a = mx \pm c$ ,  $b = nx \pm d$ , где  $|c| < x/2$ ,  $|d| < x/2$  (здесь использована нечетность  $x$ ). Число  $c^2 + 3d^2$  делится на  $x$ , скажем  $c^2 + 3d^2 = xy$ , где  $y < x$ . Ни один общий делитель чисел  $c$  и  $d$ , больший 1, не может делить  $x$ , поскольку в этом случае  $a$  и  $b$  не были бы взаимно простыми. Следовательно, обе части равенства  $c^2 + 3d^2 = xy$  можно сократить на квадрат наибольшего общего делителя  $c$  и  $d$  и получить  $e^2 + 3f^2 = xz$ , где  $e$  и  $f$  взаимно просты. Если  $x$  нельзя представить в виде  $a^2 + 3b^2$ , то, согласно (4'),  $z$  имеет нечетный делитель (обозначим его  $w$ ), который также непредставим в таком виде. Следовательно, существование нечетного числа  $x$ , делящего число вида  $a^2 + 3b^2$  (где  $a$  и  $b$  взаимно просты) и непредставимого в таком виде, влекло бы за собой существование меньшего числа  $w$  с теми же свойствами. По принципу бесконечного спуска отсюда следует требуемое заключение.

Каждое простое, кроме 3, имеет вид  $3n + 1$  или  $3n + 2$ . Число вида  $3n + 2$  нельзя представить в виде  $a^2 + 3b^2$ . Действительно, если  $a^2 + 3b^2$  не делится на 3, то  $a$  не делится на 3,  $a = 3t \pm 1$ , и  $a^2 + 3b^2$  на 1 больше некоторого кратного числа 3. Таким образом, согласно (5'), нечетное простое, которое делит число вида

$a^2 + 3b^2$  при взаимно простых  $a$  и  $b$ , не представляется в виде  $3n + 2$ . Если  $a$  и  $b$  не взаимно просты, то  $a^2 + 3b^2 = d^2(e^2 + 3f^2)$ , где  $d$  — их наибольший общий делитель и числа  $e$  и  $f$  взаимно просты. Таким образом, число вида  $a^2 + 3b^2$  можно записать в виде произведения квадрата на число, не имеющее нечетных простых делителей вида  $3n + 2$ . Согласно (2'), входящая в разложение  $a^2 + 3b^2$  степень простого числа 2 является некоторой степенью числа 4 и, следовательно, квадратом. Таким образом, *необходимое условие представимости данного числа в виде  $a^2 + 3b^2$  состоит в том, что частное от деления этого числа на наибольший содержащийся в нем квадрат не имеет простых множителей вида  $3n + 2$* . Для доказательства достаточности этого условия нужно только доказать следующее:

(6') *Каждое простое вида  $3n + 1$  представимо в виде  $a^2 + 3b^2$* . Как и раньше, по теореме Ферма, простое  $p = 3n + 1$  делит  $p - 2$  разности чисел  $1, 2^{3n}, 3^{3n}, \dots, (p - 1)^{3n}$ . Каждую из этих разностей можно разложить на множители:  $a^{3n} - b^{3n} = (a^n - b^n) \times \times (a^{2n} + a^n b^n + b^{2n})$ . Поскольку  $a$  или  $b$  четно, второй множитель можно записать в виде  $A^2 + A(2B) + (2B)^2 = (A + B)^2 + 3B^2$  со взаимно простыми  $A$  и  $B$ . Следовательно, согласно (5'), если  $p$  не делит  $p - 2$  разности чисел  $1, 2^n, 3^n, \dots, (p - 1)^n$ , то оно обязательно имеет вид  $c^2 + 3d^2$ . Если бы  $p$  делило  $p - 2$  разности этих чисел, то оно делило бы и  $n!$ , что невозможно. Следовательно,  $p$  должно иметь вид  $c^2 + 3d^2$ , что и требовалось доказать.

Применение тех же рассуждений к представлениям в виде  $a^2 + 2b^2$  позволяет доказать следующее утверждение: *для того чтобы данное число было представимо в виде  $a^2 + 2b^2$ , необходимо, чтобы частное от деления этого числа на наибольший содержащийся в нем квадрат не имело простых делителей вида  $8n + 5$  или  $8n + 7$* . Для доказательства достаточности этого условия нужно только показать, что все простые вида  $8n + 1$  или  $8n + 3$  можно представить в виде  $a^2 + 2b^2$ . Именно это последнее утверждение, аналогичное (6'), Эйлеру не удалось доказать; впервые его доказал Лагранж. (Доказательство приведено ниже в упр. 6 и 7.)

## Упражнения

1. Предположим, что некоторое простое представимо в виде  $a^2 + b^2$ . Докажите единственность такого представления. [Используйте доказательство утверждения (2).] Справедливо ли это утверждение для простых вида  $a^2 + 2b^2$  или  $a^2 + 3b^2$ ?

2. Докажите, что  $n$ -е разности от  $x^n$  равны  $n!$  (и, следовательно, все более высокие разности тождественно равны нулю). [Докажите, что первая разность от многочлена  $n$ -й степени является многочленом  $(n - 1)$ -й степени.]

3. Используя арифметику иррациональностей, получите формулу  $(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$ . Прделайте то же самое и выведите аналогичную формулу для чисел вида  $a^2 + kb^2$ .



4. Докажите, что каждый делитель числа вида  $a^2 - 2b^2$  при взаимно простых  $a$  и  $b$  представим в таком же виде  $c^2 - 2d^2$ .

5. В § 1.7 было замечено, что 21 представимо в виде  $a^2 + 5b^2$ , но ни 3, ни 7 не представимы в таком виде. Найдите, в каком месте перестают работать методы данного параграфа, если попытаться применить их для доказательства утверждения, согласно которому каждый делитель данного числа вида  $a^2 + 5b^2$  со взаимно простыми  $a$  и  $b$  представим в виде  $c^2 + 5d^2$ .

6. Следующим образом докажите, что каждое простое вида  $8n + 3$  представимо в виде  $a^2 + 2b^2$ . Пусть  $p = 8n + 3$  — простое число. Через  $x$  обозначим целое  $(p + 1)/2$ . Так как  $x^{8n+2} - 1$  делится на  $p$ , то  $x^{8n} (p + 1)^2 - 4$  делится на  $p$  и, следовательно,  $(x^{4n} - 2)(x^{4n} + 2)$  делится на  $p$ . Используя упр. 4, покажите, что  $p$  не может делить  $x^{4n} - 2$ . Следовательно,  $p$  делит  $x^{4n} + 2$ . Заключите отсюда, что  $p = a^2 + 2b^2$ .

7. Следующим образом докажите, что каждое простое вида  $8n + 1$  представимо в виде  $a^2 + 2b^2$ . Пусть  $p = 8n + 1$  — простое. Последовательные разности чисел  $1, 2^{8n}, 3^{8n}, 4^{8n}, \dots$  можно разложить в произведения  $a^{8n} - b^{8n} = (a^{4n} - b^{4n})(a^{4n} + b^{4n})$ , и второй множитель можно записать в виде  $(a^{2n} - b^{2n})^2 + 2(a^n b^n)^2$ . Доказательство получается из этих замечаний при помощи методов данного параграфа.

8. Покажите, что эйлерово доказательство утверждения (2) можно получить при попытке произвести деление  $(a + b\sqrt{-1})/(p \pm q\sqrt{-1})$ .

9. Дайте другое доказательство утверждения (5), показав, что сравнение  $(x + 1)^{2n} - x^{2n} \equiv 0 \pmod{p}$  имеет не более  $2n$  различных корней по модулю  $p$  (в действительности число корней не превосходит  $2n - 1$ ). Вообще, если хотя бы один коэффициент многочлена  $f(x)$  степени  $m$  не сравним с нулем по модулю  $p$ , то сравнение  $f(x) \equiv 0 \pmod{p}$  имеет не более  $m$  различных решений. [Не ограничивая общности, можно предположить, что старший коэффициент  $f(x)$  не сравним с нулем по модулю  $p$ . Если  $r$  — произвольное решение сравнения  $f(r) \equiv 0 \pmod{p}$ , то  $f(x) = (x - r)q(x) + c$ , где  $q(x)$  — многочлен степени  $m - 1$ , старший коэффициент которого совпадает со старшим коэффициентом многочлена  $f(x)$ , а  $c$  — целое число, сравнимое с нулем по модулю  $p$ . Каждое решение  $s$  сравнения  $f(s) \equiv 0 \pmod{p}$  (за возможным исключением  $s = r$ ) является решением сравнения  $q(s) \equiv 0 \pmod{p}$ . При  $m = 0$  доказываемое предложение, очевидно, справедливо.]

10. В § 1.8 было указано, что все простые делители числа  $2^{32} + 1$  сравнимы с 1 по модулю 64, так что 641 является только пятым простым, которое может делить  $2^{32} + 1$ . Покажите, что в действительности простые делители числа  $2^{32} + 1$  должны быть сравнимы с 1 по модулю 128, так что 641 — только второе простое число, подлежащее рассмотрению. [Пусть  $p$  — простой делитель числа  $2^{32} + 1$ . Так как  $p \equiv 1 \pmod{64}$ , то  $p$  делит  $x^2 - 2$  для некоторого  $x$ . Но  $x^{p-1} \equiv 1 \pmod{p}$ , поэтому предыдущие рассуждения показывают, что 64 делит  $(p - 1)/2$ .]

11. Разложите  $2^{32} - 1$  на простые делители и получите отсюда, что 257 не делит  $2^{32} + 1$ . [Здесь не требуется никаких вычислений.]

## 2.5. Завершение доказательства Последней теоремы Ферма при $n = 3$

Идея Эйлера проводить вычисления с «числами» вида  $a + b\sqrt{-c}$  тесно связана с использованием формулы

$$(x^2 + cy^2)(u^2 + cv^2) = (xu - cyv)^2 + c(xv + yu)^2,$$

которая неоднократно встречалась выше. Эта формула утверждает следующее. Предположим, что целое число  $A$  является произве-



дением целых  $B$  и  $C$ , представимых в виде  $a^2 + cb^2$ , скажем  $B = x^2 + cy^2$ ,  $C = u^2 + cv^2$ . Тогда  $A$  тоже можно записать в таком виде, используя для нахождения  $a$  и  $b$  формулу  $a + b\sqrt{-c} = (x + y\sqrt{-c})(u + v\sqrt{-c})$ .

Лемма, необходимая для доказательства Последней теоремы Ферма при  $n = 3$ , утверждает, что если  $a$  и  $b$  взаимно просты и  $a^2 + 3b^2$  является кубом, то  $a + b\sqrt{-3} = (p + q\sqrt{-3})^3$  при некоторых целых  $p$  и  $q$ . Для доказательства этого утверждения естественно продолжить рассуждения Эйлера лишь на один шаг дальше и «разложить»  $a + b\sqrt{-3}$  следующим образом.

(1) Если  $a$  и  $b$  взаимно просты и  $a^2 + 3b^2$  — четное число, то  $a + b\sqrt{-3}$  можно записать в виде

$$a + b\sqrt{-3} = (1 \pm \sqrt{-3})(u + v\sqrt{-3})$$

при соответствующем выборе знака и целых  $u$ ,  $v$ . Поскольку  $a^2 + 3b^2$  четно,  $a$  и  $b$  должны быть числами одинаковой четности; но они взаимно просты, следовательно, они должны быть нечетными. Таким образом, каждое из них имеет вид  $4n \pm 1$  и либо  $a + b$ , либо  $a - b$  делится на 4. Если  $a + b$  делится на 4, то равенство  $4(a^2 + 3b^2) = (1^2 + 3 \cdot 1^2)(a^2 + 3b^2) = (a - 3b)^2 + 3 \times \times (a + b)^2$  можно разделить на  $4^2$  и представить  $(a^2 + 3b^2)/4$  в виде  $u^2 + 3v^2$ , где  $u = (a - 3b)/4$ ,  $v = (a + b)/4$ . Заметим, что последние соотношения эквивалентны равенству  $u + v\sqrt{-3} = (a + b\sqrt{-3})(1 + \sqrt{-3})/4$ ; поэтому они позволяют выразить  $a$  и  $b$  через  $u$  и  $v$  и получить, как и требуется,  $(1 - \sqrt{-3}) \times \times (u + v\sqrt{-3}) = a + b\sqrt{-3}$ . Аналогично, если  $a - b$  делится на 4, то  $a + b\sqrt{-3} = (1 + \sqrt{-3})(u + v\sqrt{-3})$  при подходящих  $u$  и  $v$ . При этом  $u$  и  $v$  взаимно просты (поскольку в противном случае  $a$  и  $b$  не были бы взаимно простыми) и  $a^2 + 3b^2 = 4(u^2 + 3v^2)$ .

(2) Если  $a$  и  $b$  взаимно просты и  $a^2 + 3b^2$  делится на нечетное простое  $P$ , то  $P$  можно представить в виде  $P = p^2 + 3q^2$  с положительными целыми  $p$  и  $q$ , а  $a + b\sqrt{-3}$  представимо в виде  $a + b\sqrt{-3} = (p \pm q\sqrt{-3})(u + v\sqrt{-3})$  при соответствующем выборе знака и целых  $u$  и  $v$ . Первое утверждение, согласно которому  $P = p^2 + 3q^2$ , совпадает с утверждением (5') из предыдущего параграфа. Как и в доказательстве Эйлера, либо  $pb + aq$ , либо  $pb - aq$  делится на  $P$ . Если  $pb + aq$  делится на  $P$ , то обе части равенства  $P(a^2 + 3b^2) = (p^2 + 3q^2)(a^2 + 3b^2) = (pa - 3qb)^2 + 3(pb + aq)^2$  можно разделить на  $P^2$  и записать  $(a^2 + 3b^2)/P$  в виде  $u^2 + 3v^2$ , где  $u = (pa - 3qb)/P$  и  $v = (pb + aq)/P$ , т. е.

$$u + v\sqrt{-3} = (p + q\sqrt{-3})(a + b\sqrt{-3})/P.$$

Тогда умножение на  $p - q\sqrt{-3}$ , как и требуется, дает  $(p - q\sqrt{-3})(u + v\sqrt{-3}) = a + b\sqrt{-3}$ . Аналогично, если  $pb - aq$  делится на  $P$ , то  $a + b\sqrt{-3} = (p + q\sqrt{-3})(u + v\sqrt{-3})$ . Здесь снова  $u$  и  $v$  взаимно просты и  $a^2 + 3b^2 = P(u^2 + 3v^2)$ .

(3) Пусть  $a$  и  $b$  взаимно просты. Тогда  $a + b\sqrt{-3}$  можно записать в виде

$$a + b\sqrt{-3} = \pm (p_1 \pm q_1\sqrt{-3})(p_2 \pm q_2\sqrt{-3}) \dots (p_n \pm q_n\sqrt{-3}),$$

где  $p_i$  и  $q_i$  — положительные целые и  $p_i^2 + 3q_i^2$  равно либо 4, либо нечетному простому числу. Если  $a^2 + 3b^2$  четно, то оно делится на 4. Если  $a^2 + 3b^2 \neq 1$ , то это число имеет делитель  $P$ , равный либо 4, либо нечетному простому, и из утверждения (1) или (2) следует, что  $a + b\sqrt{-3} = (p \pm q\sqrt{-3})(u + v\sqrt{-3})$ , где  $p^2 + 3q^2 = P$ . Тогда  $u$  и  $v$  взаимно просты, и задача выделения множителя  $p \pm q\sqrt{-3}$  из  $u + v\sqrt{-3}$  совпадает с задачей выделения такого множителя из  $a + b\sqrt{-3}$ , за исключением того обстоятельства, что  $u^2 + 3v^2 = (a^2 + 3b^2)/P$  меньше  $a^2 + 3b^2$ . Повторение этого процесса приведет в конце концов к выражению вида

$$a + b\sqrt{-3} = (p_1 \pm q_1\sqrt{-3}) \dots (p_n \pm q_n\sqrt{-3})(u + v\sqrt{-3}),$$

где  $u^2 + 3v^2 = 1$ . Тогда  $u = \pm 1$ ,  $v = 0$ ,  $u + v\sqrt{-3} = \pm 1$ , и разложение завершено.

(4) Пусть  $a$  и  $b$  взаимно просты. Тогда множители в приведенном выше разложении  $a + b\sqrt{-3}$  однозначно определены (с точностью до выбора знаков) тем обстоятельством, что  $(p_1^2 + 3q_1^2) \times \dots \times (p_n^2 + 3q_n^2) = a^2 + 3b^2$  является разложением  $a^2 + 3b^2$  на нечетные простые множители и множители, равные 4. Кроме того, в это разложение может входить только один из множителей  $p + q\sqrt{-3}$  или  $p - q\sqrt{-3}$ . Для доказательства первого утверждения следует показать, что  $p^2 + 3q^2 = P$  определяет  $p$  и  $q$  с точностью до знака; здесь  $P = 4$  или  $P$  — нечетное простое. При  $P = 4$  это утверждение очевидно. Пусть  $P$  — нечетное простое. Если бы  $a^2 + 3b^2$  было другим представлением простого  $P$ , то, согласно (2),

$$a + b\sqrt{-3} = (p \pm q\sqrt{-3})(u + v\sqrt{-3})$$

и  $P = P(u^2 + 3v^2)$ , т. е.  $u^2 + 3v^2 = 1$ ,  $u = \pm 1$ ,  $v = 0$ ,  $a + b\sqrt{-3} = \pm (p \pm q\sqrt{-3})$ , что и требовалось показать. Второе утверждение следует из того, что множители  $p + q\sqrt{-3}$  и  $p - q\sqrt{-3}$  в произведении давали бы множитель  $p^2 + 3q^2$ , а это при взаимно простых  $a$  и  $b$  невозможно.

Теперь легко доказать лемму, которая требуется для завершения эйлерова доказательства Последней теоремы Ферма при  $n = 3$ .

**Лемма.** Пусть  $a$  и  $b$  — такие взаимно простые числа, что  $a^2 + 3b^2$  является кубом. Тогда существуют такие целые  $p$  и  $q$ , что  $a + b\sqrt{-3} = (p + q\sqrt{-3})^3$ .

**Доказательство.** Пусть  $a^2 + 3b^2 = P_1 P_2 \dots P_n$  — такое разложение числа  $a^2 + 3b^2$  на множители, равные нечетным простым или 4, как в утверждении (4). Если это разложение содержит в точности  $k$  множителей, равных 4, то  $2^{2k}$  является наибольшей степенью числа 2, которая делит  $a^2 + 3b^2$ , а поскольку  $a^2 + 3b^2$  является кубом, отсюда следует, что  $2k$ , а потому и  $k$  делятся на 3. Кроме того, любое нечетное простое  $P$  должно входить в это разложение с кратностью, делящейся на 3. Следовательно,  $n$  делится на 3 и множители  $P_1, P_2, \dots, P_n$  можно сгруппировать таким образом, что  $P_{3k+1} = P_{3k+2} = P_{3k+3}$ . Отсюда вытекает, что в разложении числа  $a + b\sqrt{-3}$ , полученном в утверждении (3), множители, соответствующие каждой группе из трех чисел  $P$ , совпадают, поскольку единственной альтернативой является выбор знака в  $p \pm q\sqrt{-3}$ , а числа с различными знаками не могут одновременно входить в это разложение. Если из каждой такой группы из трех множителей выбрать один и выбранные числа перемножить, то мы получим такое число  $c + d\sqrt{-3}$ , что  $a + b\sqrt{-3} = \pm(c + d\sqrt{-3})^3$ . Так как  $-(c + d\sqrt{-3})^3 = (-c - d\sqrt{-3})^3$ , отсюда следует требуемое заключение.

## Упражнения

1. Для доказательства следующего утверждения требуется только незначительная модификация проведенных выше рассуждений. Пусть  $a$  и  $b$  — взаимно простые числа; предположим, что  $a^2 + 2b^2$  является кубом. Тогда существуют такие целые  $p$  и  $q$ , что  $a + b\sqrt{-2} = (p + q\sqrt{-2})^3$ . Используйте это предположение для доказательства утверждения Ферма, согласно которому единственным решением уравнения  $x^2 + 2 = y^3$  в целых числах является  $5^2 + 2 = 3^3$ .

2. Аналогично, пусть  $a$  и  $b$  взаимно просты; предположим, что  $a^2 + b^2$  является кубом. Докажите, что  $a + b\sqrt{-1} = (p + q\sqrt{-1})^3$ . Доказательство этого утверждения при  $a = 0, b = 1$  требует особого внимания. Докажите, что единственным решением уравнения  $x^2 + 4 = y^3$  в целых числах при нечетном  $x$  является  $11^2 + 4 = 5^3$ . [Это доказательство и доказательство упр. 1, по существу, предложены Эйлером, однако Эйлер, кажется, не заметил того, что этот метод решения уравнения  $a^2 + b^2 = \text{куб}$  предполагает взаимную простоту  $a$  и  $b$ . Поэтому его доказательство того, что  $x = 4, 11$  являются единственными решениями уравнения  $x^2 + 4 = y^3$ , неполно.]

3. Дополните доказательство утверждения о том, что  $11^2 + 4 = 5^3$  и  $2^2 + 4 = 3^3$  являются единственными решениями уравнения  $x^2 + 4 = y^3$ , доказав, что если  $x^2 + 4 = y^3$  и  $x$  четно, то  $x = \pm 2$ . [Данное уравнение приводит к уравнению  $u^2 + 1 = 2v^3$ . Используйте деление числа  $u + \sqrt{-1}$  на  $1 + \sqrt{-1}$  для того, чтобы записать  $v^3 = (u^2 + 1)/2$  в виде суммы двух квадратов, скажем  $a^2 + b^2$ . Поскольку  $a$  и  $b$  отличаются на 1, они взаимно

просты и можно получить равенство  $1 = (p + q)(p^2 - 4pq + q^2)$ , где  $p$  и  $q$  целые. Таким образом,  $p + q = p^2 - 4pq + q^2 = \pm 1$  и  $-6pq = 0$  или  $-2$ . Следовательно,  $p$  или  $q$  должно равняться 0, что приводит к  $x = \pm 2$ .]

4. Докажите, что в утверждении (3) самое большее одно из чисел  $p_i^2 + 3q_i^4$  равно 4.

5. Найдите все представления в виде  $a^2 + 3b^2$  ( $a, b$  — не обязательно взаимно простые) следующих чисел: (a) 91; (b) 49; (c) 336.

## 2.6. Дополнение о суммах двух квадратов

В одном письме от 1654 г. Паскалю [F3], которое почти наверное не было известно Эйлеру, Ферма сформулировал некоторые свои теоремы, среди которых была теорема о представимости каждого простого числа вида  $4n + 1$  в виде суммы двух квадратов. Список приведенных в этом письме теорем почти совпадает со списком теорем из упомянутого выше письма к Дигби (§ 2.4), однако есть и важное различие. В письме к Паскалю Ферма дополнительно ставит задачу *нахождения* разложений в виде суммы двух квадратов, а именно: «для любого данного простого числа такого вида, скажем 53, найти *по общему правилу* два квадрата, из которых это число составлено» (курсив наш). Конечно, такое разложение всегда можно найти методом проб и ошибок (в примере Ферма решение таким методом:  $53 = 4 + 49$  — получается почти мгновенно). Ясно, однако, что Ферма придавал особую важность нахождению более методичного и эффективного способа.

Доказательство Эйлера является косвенным; оно использует рассуждение от противного, которое показывает, что если бы простое число вида  $4n + 1$  не было суммой двух квадратов, то можно было бы указать бесконечно убывающую последовательность положительных целых чисел. Следовательно, это доказательство не решает предложенную Ферма задачу нахождения конструктивного метода. Однако, как часто бывает в таких ситуациях, более тщательный анализ этого доказательства от противного показывает, что его можно видоизменить и получить конструктивное доказательство, причем эта модификация придает и самому доказательству большую ясность.

Предложение (5) из доказательства Эйлера вполне конструктивно. В нем утверждается, что для простого числа  $4n + 1$  по крайней мере одно из чисел  $1^{2n} + 2^{2n}, 2^{2n} + 3^{2n}, \dots, (4n - 1)^{2n} + (4n)^{2n}$  делится на  $4n + 1$ . В примере Ферма  $4n + 1 = 53$  легко проверить, что уже первое число  $1 + 2^{26}$  из этого списка делится на 53. В обозначениях для сравнений<sup>1)</sup> находим:  $2^6 = 64 \equiv 11 \pmod{53}$ ,  $2^{12} \equiv 11^2 = 121 \equiv 15 \pmod{53}$ ,  $2^{13} \equiv 2 \cdot 15 = 30 \pmod{53}$ ,  $2^{26} \equiv 900 \equiv -1 \pmod{53}$ ; следовательно,  $2^{26} + 1$  делится на 53. То обстоятельство, что 53 делит  $2^{26} + 1$ , используется в доказательстве Эйлера для того, чтобы показать,

<sup>1)</sup> См. приложение, § A.1.

что 53 делит сумму двух квадратов. Приведенные выше вычисления дают в явном виде сумму двух квадратов, делящуюся на 53, а именно  $30^2 + 1 = 17 \cdot 53$ . В предложении (4) Эйлер приходит к заключению, что 53 должно быть суммой двух квадратов, поскольку в противном случае возникла бы конструкция бесконечного спуска. Задача состоит в том, чтобы дать прямое доказательство этого утверждения, не прибегая к доказательству от противного.

В общем случае при  $p = 4n + 1$  методом Эйлера можно найти представление  $a^2 + b^2 = kp$ , где  $a$  и  $b$  взаимно просты и  $k < p$ . Грубо говоря, задача состоит в том, чтобы найти какой-нибудь способ, позволяющий сократить обе части этого равенства на  $k$ . Эйлерово доказательство утверждения (2) показывает, как делить на *простые* числа, которые являются суммами двух квадратов. Легко показать, что каждый простой делитель числа  $a^2 + b^2$  либо равен 2, либо имеет вид  $4n + 1$  (см. упр. 2 из § 1.8); поэтому можно делить на  $k$ , если разложить число  $k$  на простые множители, представить каждый такой множитель в виде суммы двух квадратов и делить на каждый такой множитель в отдельности. В рассматриваемом случае число  $k = 17$  само является простым, и его очень легко записать в виде суммы двух квадратов, а именно  $17 = 1^2 + 4^2$ . Процесс деления состоит в том, чтобы записать  $17 \cdot 17 \cdot 53 = (1^2 + 4^2)(30^2 + 1^2) = (30 \mp 4)^2 + (1 \pm 120)^2$  и выбрать знаки таким образом, чтобы сделать возможным деление на 17. Как и требуется, это дает  $53 = (34/17)^2 + (119/17)^2 = 2^2 + 7^2$ .

Этот метод сводит задачу представления простого числа  $p$  в виде суммы двух квадратов к задаче представления меньших простых вида  $4n + 1$ , а именно простых делителей числа  $k$ , в виде суммы двух квадратов. Возможно, это и есть тот самый метод, который имел в виду Ферма, когда описывал свое доказательство при помощи бесконечного спуска следующими словами: «Если бы выбранное простое число, которое на единицу больше некоторого числа, делящегося на 4, не было суммой двух квадратов, то существовало бы простое число такой же природы, меньшее заданного, а затем еще и третье, и т. д., бесконечно убывая до тех пор, пока не будет достигнуто простое число 5, которое является наименьшим из всех чисел такой природы; отсюда следовало бы, что 5 не является суммой двух квадратов, что не соответствует действительности. Отсюда сведением к абсурду следует заключить, что все числа такой природы являются суммами двух квадратов». (Письмо к Каркави [F5].)

Однако этот метод приводит к очень длинным вычислениям, так как требуется определить, будет ли число  $k$  простым (что всегда является трудным процессом), разложить его на множители (если это возможно) и представить каждый множитель в виде суммы двух



квадратов. В общем случае значительно лучший метод состоит в сокращении на  $k$  ценой умножения на некоторое меньшее число  $n$  (вместо  $k$ ). Это можно сделать следующим образом. Как и в эйлеровом доказательстве утверждения (4), воспользуемся равенством  $a^2 + b^2 = kp$  для нахождения меньшего числа, кратного  $p$  и представимого в виде суммы двух квадратов. Для этого запишем  $a = q_1k \pm c$ ,  $b = q_2k \pm d$  и заметим, что  $k$  должно делить  $c^2 + d^2$ , скажем  $c^2 + d^2 = nk$ . Поскольку  $|c| \leq k/2$ ,  $|d| \leq k/2$ , мы получаем, как и раньше, что  $n \leq k/2$ . Кроме того,  $nkkr = (c^2 + d^2) \times \times (a^2 + b^2) = (ca \mp db)^2 + (cb \pm da)^2$ . Наша цель состоит в том, чтобы разделить обе части этого равенства на  $k^2$ . Поскольку  $k$  не обязательно простое, здесь нельзя применить использованный раньше метод доказательства делимости  $cb + da$  или  $cb - da$  на  $k$ . Однако можно воспользоваться более простым методом. Заметим, что  $cb \pm da = c(q_2k \pm d) \pm d(q_1k \pm c)$  делится на  $k$ , если знаки выбрать таким образом, что слагаемые  $\pm cd \pm dc$  взаимно уничтожаются. Следовательно, обе части этого равенства можно разделить на  $k^2$ , что приведет к представлению  $nr$  в виде суммы двух квадратов. Если  $n = 1$ , то  $p$  уже записано в виде суммы двух квадратов. В противном случае этот процесс можно повторить и получить целое число  $m \leq n/2$  и представление  $mr$  в виде суммы двух квадратов. Продолжая этот процесс, мы должны в конце концов прийти к представлению  $p$  в виде суммы двух квадратов.

В примере  $30^2 + 1^2 = 17 \cdot 53$  имеем  $c = -4$ ,  $d = 1$ ,  $4^2 + 1^2 = 17$ , и это тот же процесс, что и выше. В качестве второго примера рассмотрим случай  $p = 229$ . На первом шаге надо вычислить  $2^{114}$  по модулю 229. Здесь  $2^8 = 256 \equiv 27 \pmod{229}$ ;  $2^{16} \equiv 27^2 \equiv 729 \equiv 42 \pmod{229}$ ;  $2^{32} \equiv 42^2 = 1764 \equiv -68 \pmod{229}$ ;  $2^{64} \equiv 68^2 = 4624 \equiv 44 \pmod{229}$ ;  $2^{96} \equiv (-68)(44) = -2992 \equiv -15 \pmod{229}$ ;  $2^{112} \equiv (-15)(42) = -630 \equiv 57 \pmod{229}$ ;  $2^{114} \equiv 4 \cdot 57 \equiv -1 \pmod{229}$ . Следовательно, 229 делит  $(2^{57})^2 + 1^2$ , и в дальнейших вычислениях нет необходимости. Затем найдем  $2^{57}$  по модулю 229:  $2^{48} \equiv (-68)(42) = -2856 \equiv -108$ ;  $2^{56} \equiv (-108)(27) = -2916 \equiv -168 \equiv 61$ ; наконец,  $2^{57} \equiv 122 \pmod{229}$ . Теперь прямое вычисление дает  $122^2 + 1 = 65 \cdot 229$ , что служит началом процесса. На первом шаге  $c = 122 - 2 \cdot 65 = -8$  и  $d = 1$ , поэтому  $8^2 + 1^2 = 65$ . Тогда  $65 \cdot 65 \cdot 229 = (8^2 + 1^2)(122^2 + 1^2) = (976 \mp 1)^2 + (8 \pm 122)^2$ , откуда  $229 = (975/65)^2 + (130/65)^2 = 15^2 + 2^2$ <sup>1)</sup>.

Совершенно аналогичную процедуру можно использовать для нахождения представления простого числа вида  $3n + 1$  в виде  $a^2 + 3b^2$ . На первом шаге надо найти  $2^n$  по модулю  $p$ . Если  $2^n$  на единицу больше некоторого кратного  $p$ , то  $p$  делит  $2^n - 1$  и следует вычислить  $3^n$  по модулю  $p$ . В конце концов мы должны

<sup>1)</sup> Другой метод решения уравнения  $p = a^2 + b^2$  указан в упр. 9 к § 7.10.



прийти к такому целому  $c$ , что  $c^n$  не является числом, на единицу большим некоторого кратного  $p$ , но этим свойством обладает  $(c - 1)^n$ . Тогда, поскольку  $p$  делит  $c^{3n} - (c - 1)^{3n}$ , то  $p$  должно делить  $c^{2n} + c^n (c - 1)^n + (c - 1)^{2n}$ ; последнее число имеет вид  $a^2 + 3b^2$ . Таким образом,  $a^2 + 3b^2 = kp$ , и можно добиться выполнения неравенства  $k \leq p$ . Если  $a$  и  $b$  четны, то их можно сократить на степени числа 2. Если оба они нечетны, то 4 делит  $a^2 + 3b^2$ , и можно воспользоваться следующим методом сокращения на 4:  $\frac{a^2 + 3b^2}{4} = \left(\frac{a \mp 3b}{4}\right)^2 + 3\left(\frac{a \pm b}{4}\right)^2$ , где знаки выбраны таким образом, что 4 делит  $a \pm b$ . Это сводит задачу к случаю  $a^2 + 3b^2 = kp$ , где  $a$  и  $b$  — числа противоположной четности. Если  $k = 1$ , то задача решена. В противном случае  $a$  можно привести к  $c$  по модулю  $k$ , а  $b$  привести к  $d$  и получить  $c^2 + 3d^2 = nk$ , где  $n < k$  (поскольку  $k$  нечетно). Тогда при соответствующем выборе знаков можно сократить обе части равенства  $nkkp = (ac \mp 3bd)^2 + 3(ad \pm bc)^2$  на  $k^2$  и получить  $np = e^2 + 3f^2$ . Если  $n \neq 1$ , то можно снова воспользоваться приведением — до тех пор, пока мы не получим  $p = g^2 + 3h^2$ .

Например, рассмотрим случай  $p = 67$ . На первом шаге надо вычислить  $2^{22}$  по модулю 67. Это очень просто:  $2^6 = 64 \equiv -3$ ,  $2^{12} \equiv 9$ ,  $2^{18} \equiv -27$ ,  $2^{19} \equiv -54 \equiv 13$ ,  $2^{21} \equiv 52 \equiv -15$ ,  $2^{22} \equiv -30$ . Таким образом,  $2^{22} - 1$  не делится на 67, а  $2^{44} + 2^{22} + 1$  должно делиться. Но  $2^{44} + 2^{22} + 1 = 3\left(\frac{1}{2}2^{22}\right)^2 + \left(\frac{1}{2}2^{22} + 1\right)^2 = 3(2^{21})^2 + (2^{21} + 1)^2$ . Поскольку  $2^{21} \equiv -15$ , отсюда следует, что  $3 \cdot (-15)^2 + (-14)^2$  должно делиться на 67. Прямое вычисление дает:  $3 \cdot 15^2 + 14^2 = 871 = 13 \cdot 67$ . Приводя 15 и 14 по модулю 13, получаем  $3 \cdot 2^2 + 1^2 \equiv 0 \pmod{13}$ ; в действительности  $3 \cdot 2^2 + 1^2 = 13$ . Следовательно,  $13 \cdot 13 \cdot 67 = (1^2 + 3 \cdot 2^2)(14^2 + 3 \cdot 15^2) = (14 \mp 3 \cdot 30)^2 + 3(15 \pm 28)^2$ ,  $67 = (104/13)^2 + 3(-13/13)^2 = 8^2 + 3 \cdot 1^2$ .

Последняя часть этой процедуры применима в случае задачи представления простых в виде  $a^2 + 2b^2$ . Если можно найти число вида  $a^2 + 2b^2$ , делящееся на  $p$ , то аналогичная процедура позволяет найти представление самого числа  $p$  в таком виде. При этом недостает лишь метода построения при данном простом  $p$  вида  $p = 8n + 1$  или  $p = 8n + 3$  числа вида  $a^2 + 2b^2$ , делящегося на  $p$ . Конструктивный метод такого построения приведен в упр. 6 и 7 к § 2.4.

### Упражнения

1. Запишите 97 в каждой из трех форм  $a^2 + b^2$ ,  $a^2 + 3b^2$ ,  $a^2 + 2b^2$ .
2. Запишите 193 в каждой из трех форм упр. 1.
3. Запишите 7297 во всех трех формах.
4. В статье Якоби [J1] содержатся обширные таблицы представления простых в виде  $a^2 + b^2$ ,  $a^2 + 2b^2$  и  $a^2 + 3b^2$ . Просмотрите эти таблицы и выведите несколько приведенных в них представлений.

## Глава 3

# ОТ ЭЙЛЕРА ДО КУММЕРА

### 3.1. Введение

Когда Эйлер в письме Гольдбаху от 4 авг. 1753 г. говорил, что ему удалось доказать Последнюю теорему Ферма в случае  $n = 3$ , он отметил, что это доказательство представляется ему совершенно отличным от того, которое было в случае  $n = 4$ , и что доказательство общего случая кажется весьма далеким. В последующие 90 лет было получено еще несколько — очень немного — частных случаев и частичных результатов, но общий случай все еще казался абсолютно недостижимым. Затем, в 1840-е годы, Куммер развил свою теорию идеальных делителей и с ее помощью получил новые глубокие результаты, касающиеся Последней теоремы Ферма, которые породили надежду, что и сам общий случай вскоре будет доказан.

Эта глава посвящена наиболее важным результатам, полученным в течение этого девятидесятилетнего периода. В § 3.2 формулируется и доказывается теорема Софи Жермен, § 3.3 посвящен доказательству Последней теоремы Ферма в случае  $n = 5$ , полученному Лежандром и Дирихле, а § 3.4 — несколькими замечаниями о доказательствах, которые получили Дирихле и Ламе в случаях  $n = 14$  и  $n = 7$  соответственно. Теорема Софи Жермен имеет важное значение, и хотя позже она была обобщена и улучшена, она не была ничем заменена со времени ее открытия. В то же время доказательства случаев  $n = 5$  и  $n = 7$  были заменены доказательствами Куммера Последней теоремы Ферма для «регулярных простых» (а случай  $n = 14$  — более общим случаем  $n = 7$ ). Сейчас они представляют интерес лишь как примеры того, что можно сделать более элементарными средствами, не обращаясь к теории идеальных делителей, и как развитие теории привело к великим открытиям Куммера.

Хотя на протяжении этого периода прогресс на пути к доказательству Последней теоремы Ферма был невелик, развитие теории чисел в целом достигло громадных успехов. В эту эпоху жили трое из крупнейших за всю историю теоретиков в области чисел — Лагранж, Лежандр и Гаусс.

Лагранж был уже упомянут выше как в связи с решением уравнения Пелля (§ 1.9), так и в связи с доказательством того, что каждое число может быть записано в виде суммы четырех квадра-

тов (§ 2.4). Выдающиеся способности Лагранжа были признаны Эйлером, когда Лагранж был еще совсем молод, и сотрудничество между ними было весьма плодотворным. Когда Эйлер оставил двор Фридриха Великого, чтобы в 1766 г. вернуться в Россию, Лагранж заменил его в Берлине. Более того, когда в 1783 г. Эйлер умер, Лагранж бесспорно занял его место крупнейшего европейского математика. Подобно Эйлеру, он был необычайно разносторонен. Ему принадлежат фундаментальные результаты в небесной механике, вариационном исчислении, алгебре, анализе и т. д., но, как и у Эйлера, в его работах видна особая любовь к теории чисел.

Лежандр — которого из-за имени легко спутать с Лагранжем — определенно не достиг уровня Эйлера и Лагранжа, но был прекрасным математиком, проделавшим важную работу в широком разнообразии областей, особенно в теории эллиптических функций, алгебре и теории чисел. Но еще важнее, быть может, то, что он был очень плодотворным автором, работы которого охватили большой диапазон тем и достигли широкой аудитории. Его «Теория чисел» (*Théorie des Nombres*), впервые опубликованная в 1798 г., выдержала несколько изданий и оказала глубокое влияние на математическую культуру эпохи.

Гаусс опубликовал свои великие «Арифметические исследования» (*Disquisitiones Arithmeticae*) в 1801 г. (ему было в то время 24 года) и сразу же завоевал признание <sup>1)</sup> как гений первой величины. Он также был великим универсалом — о нем говорили, что не было ни одного направления в развитии математики XIX века, которое бы он не предвидел в своей работе, — но он также считал теорию чисел — высшую арифметику, как он предпочитал называть ее, — царицей математики. В дополнение к *Disquisitiones Arithmeticae* он опубликовал два классических мемуара по биквадратичной взаимности в 1828 и 1832 гг., которые оказали большое влияние на развитие теории чисел.

Деятельность этих ученых не имеет в большей части непосредственного отношения ни к самой Последней теореме Ферма, ни к методам, которые позже были успешно применены для ее изучения. Однако косвенно их деятельность оказала очень большое влияние на развитие этих методов. Помимо общего влияния, из-за которого целое поколение математиков было воспитано в убеждении, что высшая арифметика является царицей всей математики, имеется по крайней мере два весьма частных аспекта, которые будут изучены в следующих главах. Теория идеальных делителей, развитая Куммером для исследования высших законов

---

<sup>1)</sup> 31 мая 1804 г. Лагранж [L4] писал Гауссу: «Ваши *Disquisitiones* сразу же поставили Вас в ряд лучших геометров». (В те времена «геометр» означало «чистый математик».)

взаимности, и выведенная Дирихле аналитическая формула числа классов бинарных квадратичных форм с данным детерминантом — обе выросли на почве работ этих трех теоретиков и обе стали впоследствии основой исследования Последней теоремы Ферма.

Таким образом, краткость этой главы не означает, что период от Эйлера до Куммера был малопродуктивным. Наоборот, этот период во многих отношениях был золотым веком теории чисел. Краткость этой главы означает лишь, что в течение этого периода исследование Последней теоремы Ферма отошло на задний план, пока развивались другие разделы теории чисел — главным образом бинарные квадратичные формы и законы взаимности, — что только позже принесет плоды в исследовании Последней теоремы Ферма.

### 3.2. Теорема Софи Жермен

Одной из очень немногих женщин, которым вплоть до настоящего времени удалось преодолеть предубеждение и дискриминацию, направленные на отстранение женщин от занятий высшей математикой, была Софи Жермен (1776—1831). Она вела активную переписку с Гауссом, жившим в Геттингене, и была лично знакома с Лежандром в Париже. В письмах Гауссу она вначале подписывалась мужским псевдонимом, опасаясь, что иначе Гаусс не воспринял бы ее всерьез. Как бы он поступил — неясно. Известно лишь, что она добилась его расположения, не пытаясь заинтриговать его тем фактом, что она — женщина-математик, и когда обман раскрылся, Гаусс пришел в полный восторг.

«Но как описать Вам мое восхищение и изумление, когда я увидел, что мой уважаемый корреспондент г-н Лебланк превратился в эту выдающуюся личность [Софи Жермен, которой он писал после раскрытия обмана], преподнесшую столь яркий пример того, во что, я бы сказал, трудно поверить. Склонность к абстрактным наукам вообще, а к тайнам чисел в особенности — исключительно редкое качество: это не тот предмет, который поражает каждого; захватывающее очарование этой возвышенной науки открывается только тем, кто имеет мужество углубиться в нее. Но когда особа женского пола, которой на этом тернистом пути, в соответствии с нашими обычаями и предрассудками, приходится сталкиваться с неизмеримо большими, чем мужчинам, трудностями, все же добивается успеха в преодолении этих препятствий и проникает в самые темные области исследований, — она несомненно должна обладать самым доблестным мужеством, совершенно необычайными личными качествами и высшей одаренностью. В самом деле, ничто не могло бы убедить меня столь лестным и недвусмысленным образом в том, что притягательная сила этой науки, обогатившей мою жизнь таким количеством радостей, не является плодом фантазии, как преданность, которой удостоили ее Вы». (См. [G8].)

Взаимоотношения между Гауссом и Лежандром всегда были натянутыми, и, к чести Софи Жермен, нужно сказать, что ее отношения с ними обоими были наилучшими. Именно Лежандр

сделал ее знаменитой <sup>1)</sup>, упомянув о ней в своей «Теории чисел» [L7] и присвоив ее имя очень важному результату по Последней теореме Ферма, который под ее именем известен и сейчас. Эта теорема приведена ниже, вслед за обсуждением нескольких частных вопросов.

**Теорема.** Если  $x^5 + y^5 = z^5$ , то одно из чисел  $x, y, z$  делится на 5.

**Доказательство.** Хотя Последняя теорема Ферма утверждает, что равенство  $x^5 + y^5 = z^5$  не может выполняться при *положительных* целых значениях неизвестных, нам будет здесь удобно перенести член  $z^5$  в другую часть уравнения:  $x^5 + y^5 + (-z)^5 = 0$  и сформулировать случай  $n = 5$  в более симметричной форме: «уравнение  $x^5 + y^5 + z^5 = 0$  неразрешимо в ненулевых целых числах  $x, y, z$ ». Очевидное преимущество такой формулировки заключается в том, что уравниваются роли неизвестных  $x, y, z$ . Поскольку нуль делится на 5, доказываемая сейчас теорема принимает вид: «если  $x, y, z$  — такие целые числа, что  $x^5 + y^5 + z^5 = 0$ , то одно из них делится на 5».

Первый шаг доказательства состоит в переписывании уравнения в виде

$$-x^5 = (y + z)(y^4 - y^3z + y^2z^2 - yz^3 + z^4).$$

Как обычно, будем считать, что  $x, y, z$  попарно взаимно просты ибо в противном случае общий множитель можно исключить. Тогда два сомножителя в правой части взаимно просты, поскольку если  $p$  — простое, делящее  $y + z$ , то  $y \equiv -z \pmod{p}$ ,  $y^4 - y^3z + y^2z^2 - yz^3 + z^4 \equiv 5y^4 \pmod{p}$ , и если  $p$  делит оба сомножителя, то либо  $p = 5$ , и в этом случае  $x$  делится на 5, что и требовалось доказать, либо  $p$  делит  $y$  и  $y + z$ , а в этом случае  $y$  и  $z$  не взаимно просты. Иными словами, если  $x^5 + y^5 + z^5 = 0$ , числа  $x, y, z$  попарно взаимно просты и ни одно из них не делится на 5, то  $y + z$  и  $y^4 - y^3z + y^2z^2 - yz^3 + z^4$  взаимно просты. Так как их произведение является пятой степенью:  $y^5 + z^5 = -x^5 = (-x)^5$ , то каждый из них сам должен быть пятой степенью. (На этот случай легко распространить рассуждение из § 1.4.) В силу симметрии, те же рассуждения можно применить к  $-y^5 = x^5 + z^5$  и  $-z^5 = x^5 + y^5$  и получить, что для некоторых целых чисел  $a, \alpha, b, \beta, c, \gamma$

$$y + z = a^5, \quad y^4 - y^3z + y^2z^2 - yz^3 + z^4 = \alpha^5, \quad x = -a\alpha,$$

$$z + x = b^5, \quad z^4 - z^3x + z^2x^2 - zx^3 + x^4 = \beta^5, \quad y = -b\beta,$$

$$x + y = c^5, \quad x^4 - x^3y + x^2y^2 - xy^3 + y^4 = \gamma^5, \quad z = -c\gamma.$$

Мы сейчас покажем, что это невозможно.

<sup>1)</sup> Она заслужила также премию Парижской Академии за статью по теории упругости, но, насколько мне известно, эта работа не пользовалась в дальнейшем большим успехом.

Ключом к доказательству служит простое наблюдение, что пятые степени по модулю 11 равны  $-1, 0, 1$ . Это ясно из теоремы Ферма, которая утверждает, что либо  $x \equiv 0 \pmod{11}$ , либо  $(x^5)^2 \equiv 1 \pmod{11}$ , а значит, либо  $x^5 \equiv 0$ , либо  $x^5 \equiv \pm 1$ . (Точнее, нужно заметить, что из  $y^2 \equiv 1$  вытекает  $y^2 - 1 = (y - 1) \times (y + 1) \equiv 0 \pmod{11}$ ; но, поскольку 11 — простое число, последнее означает, что либо  $y - 1 \equiv 0$ , либо  $y + 1 \equiv 0 \pmod{11}$ , т. е.  $y \equiv \pm 1$ .) Следовательно, сравнение  $x^5 + y^5 + z^5 \equiv 0 \pmod{11}$  возможно, только если либо  $x$ , либо  $y$ , либо  $z \equiv 0 \pmod{11}$ , поскольку равенство  $\pm 1 \pm 1 \pm 1 = 0$  невозможно.

Предположим, что  $x^5 + y^5 + z^5 = 0$ , где  $x, y, z$  попарно взаимно просты и не делятся на 5. Тогда, как мы установили, можно найти  $a, \alpha, b, \beta, c, \gamma$ . Одно из чисел  $x, y, z$  должно делиться на 11. Не нарушая общности, предположим, что это  $x$ . Тогда число  $2x = b^5 + c^5 + (-a)^5$  делится на 11 и одно из чисел  $a, b, c$  должно делиться на 11. Это не может быть  $b$ , поскольку  $x$  делится на 11 и отсюда вытекало бы, что  $x$  и  $z$  имеют общий делитель 11, вопреки предположению об их взаимной простоте. Аналогично, на 11 не может делиться и  $c$ . Значит,  $a$  делится на 11. Но это тоже невозможно, ибо тогда  $y \equiv -z \pmod{11}$ ,  $\alpha^5 \equiv 5y^4 \pmod{11}$ , а с другой стороны,  $x \equiv 0$ ,  $\gamma^5 \equiv y^4$ , что дает  $\alpha^5 \equiv 5\gamma^5$ . Так как по модулю 11 пятые степени равны  $0, \pm 1$ , то отсюда вытекает, что  $\alpha \equiv \gamma \equiv 0$ , вопреки предположению о взаимной простоте  $x$  и  $z$ . Это завершает доказательство теоремы.

Точно такие же рассуждения позволяют доказать более общую теорему.

**Теорема.** Если  $n$  — нечетное простое число <sup>1)</sup> и число  $2n + 1$  простое, то из  $x^n + y^n = z^n$  вытекает, что или  $x$ , или  $y$ , или  $z$  делится на  $n$ .

Таким образом, для того чтобы доказать Последнюю теорему Ферма для  $n = 5$ , или  $n = 11$ , или для многих других простых значений показателя  $n$ , достаточно доказать, что равенство  $x^n + y^n = z^n$  невозможно при дополнительном предположении: одно из чисел  $x, y, z$  делится на  $n$ , — поскольку противоположный случай уже исключен настоящей теоремой. Обычно (главным образом из-за этой теоремы) Последнюю теорему Ферма разделяют на два случая: первый, когда ни одно из трех чисел  $x, y, z$  не делится на  $n$ , и второй, когда одно и только одно из этих чисел делится на  $n$ . Эти два случая принято называть Случай I и Случай II (в указанном порядке), а приведенную выше теорему формулировать так: если  $n$  — такое нечетное простое число, что  $2n + 1$  тоже про-

<sup>1)</sup> Если  $n$  есть простое число 2, то число  $2n + 1$  простое, и теорема остается верной, как мы видели в § 1.3.



стое, то для  $n$ -х степеней верен Случай I Последней теоремы Ферма.

Как это ни удивительно, Случай I гораздо элементарнее, чем Случай II. Даже тогда, когда только что приведенная теорема не имеет места, ее небольшое видоизменение часто позволяет достичь успеха. Например, в случае  $n = 7$  число  $2n + 1 = 15$  не простое, зато простым является  $4n + 1 = 29$ . По модулю 29 все 7-е степени равны  $0, \pm 1, \pm 12$  (см. упр. 4). Значит, сравнение  $x^7 + y^7 + z^7 \equiv 0 \pmod{29}$  возможно, только если одно из этих чисел является нулем по модулю 29. Тогда использованные в доказательстве предыдущей теоремы соображения показывают, что найдутся такие целые  $\alpha$  и  $\gamma$ , что  $\alpha^7 \equiv 7\gamma^7 \pmod{29}$ , но  $\alpha \not\equiv 0 \pmod{29}$  и  $\gamma \not\equiv 0 \pmod{29}$ . Так как 29 простое, имеется <sup>1)</sup> такое целое  $g$ , что  $\gamma g \equiv 1 \pmod{29}$ ; следовательно,  $(\alpha g)^7 \equiv 7 \pmod{29}$ , вопреки тому что лишь вычеты  $0, \pm 1, \pm 12$  являются 7-ми степенями по модулю 29. Это же соображение лежит в основе теоремы Софи Жермен.

**Теорема Софи Жермен.** Пусть  $n$  — нечетное простое число. Если имеется вспомогательное простое число  $p$ , обладающее свойствами:

- (1) из  $x^n + y^n + z^n \equiv 0 \pmod{p}$  вытекает  $x \equiv 0$ , или  $y \equiv 0$ , или  $z \equiv 0 \pmod{p}$ ;
  - (2) сравнение  $x^n \equiv n \pmod{p}$  невозможно,
- то для  $n$  верен Случай I Последней теоремы Ферма.

**Доказательство.** Поскольку  $n$  нечетно, Последнюю теорему Ферма для  $n$  можно переформулировать как утверждение о невозможности равенства  $x^n + y^n + z^n = 0$  при ненулевых целых  $x, y, z$ . Тогда Случай I для  $n$  — это утверждение о невозможности равенства  $x^n + y^n + z^n = 0$  при целых числах, которые не делятся на  $n$ . Поэтому предположим, что  $n$  и  $p$  удовлетворяют условиям теоремы, а  $x, y, z$  — такие целые числа, ни одно из которых не делится на  $n$ , что  $x^n + y^n + z^n = 0$ . Нужно показать, что эти предположения ведут к противоречию.

Как обычно, можно считать, что  $x, y$  и  $z$  попарно взаимно просты. Равенство  $(-x)^n = y^n + z^n = (y + z)(y^{n-1} - y^{n-2}z + y^{n-3}z^2 - \dots + z^{n-1})$  показывает, что  $y + z$  и  $y^{n-1} - y^{n-2}z + y^{n-3}z^2 - \dots + z^{n-1}$  оба являются  $n$ -ми степенями, поскольку эти сомножители взаимно просты <sup>2)</sup>. (Если бы они оба делились на некоторое простое  $q$ , то  $y + z \equiv 0$ ,  $y^{n-1} - y^{n-2}z + \dots + z^{n-1} \equiv 0$ ,  $y \equiv -z$ ,  $ny^{n-1} \equiv 0 \pmod{q}$ , откуда  $n \equiv 0$  или

<sup>1)</sup> См. приложение, § A.1.

<sup>2)</sup> Заметим, что здесь снова, как и в § 1.3, 1.5, 1.6 и 2.2, решающую роль играет теорема: «если  $uv$  есть  $n$ -я степень, а  $u$  и  $v$  взаимно просты, то  $u$  и  $v$  оба должны быть  $n$ -ми степенями».

$y \equiv 0 \pmod{q}$ . Первое невозможно, ибо тогда  $n = q$  делило бы  $x$ , а второе невозможно, ибо тогда  $q$  делило бы как  $y$ , так и  $y + z$ .) Точно такие же разложения получаются из равенств  $(-y)^n = x^n + z^n$  и  $(-z)^n = x^n + y^n$ , а отсюда следует существование таких целых чисел  $a, \alpha, b, \beta, c, \gamma$ , что

$$\begin{aligned} y + z &= a^n, & y^{n-1} - y^{n-2}z + \dots + z^{n-1} &= \alpha^n, & x &= -a\alpha, \\ z + x &= b^n, & z^{n-1} - z^{n-2}x + \dots + x^{n-1} &= \beta^n, & y &= -b\beta, \\ x + y &= c^n, & x^{n-1} - x^{n-2}y + \dots + y^{n-1} &= \gamma^n, & z &= -c\gamma. \end{aligned}$$

Теперь рассмотрим выкладки по модулю  $p$ . Так как  $x^n + y^n + z^n \equiv 0 \pmod{p}$ , то из первого условия для  $p$  вытекает, что  $x, y$  или  $z$  должно быть нулем по модулю  $p$ . Не нарушая общности, предположим, что  $x \equiv 0 \pmod{p}$ . Тогда  $2x = b^n + c^n + (-a)^n \equiv 0 \pmod{p}$  и снова из первого условия для  $p$  следует, что  $a, b$  или  $c$  должно быть нулем по модулю  $p$ . Если бы это было  $b$  или  $c$ , то сравнение  $y = -b\beta \equiv 0$  или  $z = -c\gamma \equiv 0 \pmod{p}$  вместе со сравнением  $x \equiv 0 \pmod{p}$  противоречило бы предположению о том, что  $x, y$  и  $z$  попарно взаимно просты. Значит,  $a \equiv 0 \pmod{p}$ . Но отсюда вытекает, что  $y \equiv -z \pmod{p}$ ,  $\alpha^n \equiv ny^{n-1} \equiv n\gamma^n \pmod{p}$ . Так как  $\gamma \not\equiv 0 \pmod{p}$ , имеется такое целое число  $g$ , что  $\gamma g \equiv 1 \pmod{p}$ , откуда  $(\alpha g)^n \equiv n \pmod{p}$  вопреки второму предположению о числе  $p$ . Это противоречие и доказывает теорему Софи Жермен.

При помощи этой теоремы Софи Жермен смогла доказать Случай I для всех простых, меньших 100. Иными словами, для каждого нечетного простого  $n < 100$  ей удалось найти другое простое  $p$ , которое удовлетворяло условиям этой теоремы. Лежандр расширил этот результат на все нечетные простые, меньшие 197, а также на многие другие простые числа. После этих результатов, которые были получены даже до того, как удалось доказать Последнюю теорему Ферма в случае  $n = 5$ , стало ясно, что пришло время сосредоточить внимание на более непокорном Случае II.

## Упражнения

1. Докажите, что 7-е степени по модулю 29 суть  $0, \pm 1, \pm 12$ . [Поскольку  $2^7 \equiv -12 \pmod{29}$ , все эти 5 чисел являются 7-ми степенями. Конечно, тот факт, что среди 7-х степеней встречаются только эти числа, можно доказать простым вычислением  $3^7, 4^7, \dots, 28^7$  по модулю 29. Однако более эффективный путь — заметить, что если  $x \not\equiv 0 \pmod{29}$  является 7-й степенью, то  $x^4 - 1 \equiv 0 \pmod{29}$ . Значит, достаточно доказать, что если  $f(x)$  — полином степени  $n$  со старшим коэффициентом 1, то сравнение  $f(x) \equiv 0 \pmod{p}$  имеет не более  $n$  различных решений по модулю  $p$ . Это можно сделать, используя, как и в упр. 9 из § 2.4, теорему о делении с остатком. Иначе, можно умножить  $f(x)$  на  $(x - r_1)(x - r_2) \dots (x - r_k)$ , где  $r_i$  пробегает различные по модулю  $p$  целые, не являющиеся решениями сравнения  $f(x) \equiv 0$ . Таким способом можно было бы построить полином  $g(x)$  степени меньшей  $p$  со стар-

шим коэффициентом 1, все значения которого равны нулю по модулю  $p$ . Рассуждение Эйлера с разностями из § 2.4 показывает, что это невозможно.]

2. Докажите, что условие (1) теоремы Софи Жермен тогда и только тогда выполняется, когда набор  $n$ -х степеней по модулю  $p$  не содержит двух последовательных ненулевых (по модулю  $p$ ) целых чисел.

3. Докажите для каждого из следующих простых чисел  $n$  Случай 1 Последней теоремы Ферма, найдя другое простое  $p$ , для которого выполняются условия теоремы Софи Жермен:  $n = 13, 17, 19, 23, 29$ .

4. Докажите Случай I Последней теоремы Ферма для  $n = 5$ , рассматривая сравнения по модулю 25.

5. Покажите, что для  $n = 7$  рассуждения из упр. 4 не проходят.

6. Докажите, что из условия (2) теоремы Софи Жермен следует, что  $p = mn + 1$  для некоторого четного  $m$ . [Если  $p - 1$  и  $n$  взаимно просты, то существуют такие целые числа  $\mu$  и  $\nu$ , что  $\mu(p - 1) = \nu n + 1$ . Аналогично, существуют целые  $a$  и  $b$ , такие, что  $an = bp + 1$ . Тогда  $an \equiv 1 \pmod{p}$ ,  $a^{\nu n} n^{\nu n} \equiv 1 \pmod{p}$ ,  $n \equiv a^{\nu n} n^{\nu n+1} = a^{\nu n} n^{\mu(p-1)} \equiv (a^{\nu})^n \pmod{p}$ , поскольку  $n^{p-1} \equiv 1 \pmod{p}$  по теореме Ферма. Таким образом, если  $n$  не является  $n$ -й степенью, то  $p - 1$  и  $n$  не взаимно просты. Так как  $n$  — простое, то это означает, что  $n$  делит  $p - 1$ , т. е.  $p = mn + 1$  для некоторого  $m$ . Но  $p$  нечетно ( $x^n \equiv n \pmod{2}$  для нечетного  $n$  возможно), поэтому  $m$  четно.]

### 3.3. Случай $n = 5$

Честь доказательства Последней теоремы Ферма для пятых степеней разделили два выдающихся математика, юный Дирихле<sup>1)</sup>, который только что достиг 20 лет и как раз начинал свою блестящую карьеру, и стареющий Лежандр, которому перевалило за 70 и который был всемирно известным авторитетом в теории чисел и в анализе.

Последняя теорема Ферма для пятых степеней распадается следующим образом на два случая. Как было показано в предыдущем параграфе, если  $x, y, z$  — такие попарно взаимно простые положительные целые числа, что  $x^5 + y^5 = z^5$ , то одно из них должно делиться на 5. С другой стороны, одно из этих трех чисел, очевидно, должно делиться на 2, так как иначе данное равенство представляло бы нечетное число в виде суммы двух нечетных чисел. В этом параграфе *первым случаем* будет считаться тот, когда число, делящееся на 5, делится также и на 2, а *вторым случаем* — противоположный, когда четное число и число, делящееся на 5, различны. (Это разбиение не следует путать с разделением на Случай I и Случай II в смысле предыдущего параграфа. Для  $n = 5$  Случай I исключен, а «первый случай» и «второй случай» являются подразделениями Случая II.)

В июле 1825 г. Дирихле представил в Парижскую Академию (где Лежандр был ведущим членом) статью, в которой он дока-

<sup>1)</sup> Несмотря на свою довольно французскую по виду фамилию и на то, что в то время он жил в Париже, Дирихле был немцем. Исключая несколько лет, которые можно было бы назвать стажировкой в Париже, а также некоторые путешествия в последующие годы, он родился, вырос, получил образование и провел всю свою жизнь в Германии.

зывал, что первый случай невозможен. Его доказательство, по существу, сводилось к следующему рассуждению. Если оказалось, что  $x$  или  $y$  делится на 5, то перенесем другой член суммы  $x^n + y^n$  в правую часть равенства, так чтобы член, делящийся на 5, остался один. Так как в первом случае этот член делится также и на 2, то равенство можно привести к виду

$$u^5 \pm v^5 = w^5,$$

где  $u$ ,  $v$  и  $w$  — попарно взаимно простые положительные целые числа, причем  $w$  делится на 10. Нужно показать, что это невозможно.

Числа  $u$  и  $v$  нечетны (они взаимно просты с четным числом  $w$ ), поэтому можно следовать доказательству Эйлера случая  $n = 3$  (§ 2.2), полагая  $u + v = 2p$  и  $u - v = 2q$ . Тогда  $u = p + q$ ,  $v = p - q$  и  $u^5 \pm v^5 = (p + q)^5 \pm (p - q)^5$ , что равно либо  $2(p^5 + 10p^3q^2 + 5pq^4)$ , либо  $2(5p^4q + 10p^2q^3 + q^5)$ . Меняя, если потребуется, местами  $p$  и  $q$ , мы получим равенство вида

$$2p(p^4 + 10p^2q^2 + 5q^4) = w^5,$$

в котором  $p$  и  $q$  — взаимно простые положительные целые различной четности, а  $w$  — положительное целое, делящееся на 10. Если бы 5 не делило  $p$ , то оно не делило бы и  $p^4 + 10p^2q^2 + 5q^4$ , а значит, не делило бы  $w^5$  вопреки предположению. Следовательно,  $p$  делится на 5, скажем  $p = 5r$ , а  $q$  не делится на 5. Наше равенство принимает вид

$$5^2 \cdot 2r(q^4 + 2 \cdot 5^2 r^2 q^2 + 5^3 r^4) = w^5.$$

Произведение  $5^2 \cdot 2r$  делится на 2, 5, а также на простые делители числа  $r$ . Ни одно из этих простых чисел не делит  $q^4 + 2 \cdot 5^2 r^2 q^2 + 5^3 r^4$  (напомним, что  $5 \nmid q$  и что  $q$  и  $r$  имеют различную четность). Значит, по обычной в этой ситуации теореме получаем

$$5^2 \cdot 2r = \text{пятая степень},$$

$$q^4 + 2 \cdot 5^2 r^2 q^2 + 5^3 r^4 = \text{пятая степень}.$$

Можно воспользоваться дополнением до квадрата и привести второе из этих выражений к виду

$$(q^2 + 5^2 r^2)^2 - 5^4 r^4 + 5^3 r^4 = (q^2 + 5^2 r^2)^2 - 5(10r^2)^2 = P^2 - 5Q^2.$$

Основная идея доказательства Дирихле — попытаться следовать Эйлеру, записывая выражение  $P^2 - 5Q^2$  в виде  $(P + Q\sqrt{5}) \times (P - Q\sqrt{5})$  и стараясь показать, что  $P + Q\sqrt{5}$  должно быть пятой степенью.

Предположим на время, что такое заключение обосновано, т. е. можно показать, что имеются целые  $A$  и  $B$ , для которых

$P + Q\sqrt{5} = (A + B\sqrt{5})^5$ . Тогда

$$P = A^5 + 50A^3B^2 + 125AB^4,$$

$$Q = 5A^4B + 50A^2B^3 + 25B^5.$$

Поскольку  $Q = 10r^2$  и число  $5^2 \cdot 2r$  является пятой степенью, число  $(5^2 \cdot 2r)^2 = 5^3 \cdot 2Q$  также оказывается пятой степенью, а значит,

$$5^4 \cdot 2B [A^4 + 10A^2 \cdot B^2 + 5B^4] = \text{пятая степень.}$$

Числа  $A$  и  $B$  взаимно просты, поскольку такими являются  $P$  и  $Q$ , имеют различную четность, поскольку  $P$  и  $Q$  не могут быть оба четными, и  $A$  взаимно просто с 2 и 5, поскольку таково  $P$ . Значит,

$$5^4 \cdot 2B = \text{пятая степень,}$$

$$A^4 + 10A^2B^2 + 5B^4 = \text{пятая степень.}$$

Дополняя до квадрата два первых члена в последнем выражении, приведем его к виду  $(A^2 + 5B^2)^2 - 25B^4 + 5B^4 = (A^2 + 5B^2)^2 - 5(2B^2)^2 = C^2 - 5D^2$ . Еще раз предположим, что отсюда можно заключить о справедливости равенства  $C + D\sqrt{5} = (a + b\sqrt{5})^5$ . Тогда

$$C = a^5 + 50a^3b^2 + 125ab^4,$$

$$D = 5a^4b + 50a^2b^3 + 25b^5.$$

Так как  $D = 2B^2$  и так как  $5^4 \cdot 2B = \text{пятая степень}$ , то и число  $(5^4 \cdot 2B)^2 = 5^8 \cdot 2D$  является пятой степенью, т. е.

$$5^9 \cdot 2b [a^4 + 10a^2b^2 + 5b^4] = \text{пятая степень,}$$

откуда, как и раньше,

$$5^9 \cdot 2b = \text{пятая степень,}$$

$$a^4 + 10a^2b^2 + 5b^4 = \text{пятая степень.}$$

Первое равенство, очевидно, равносильно равенству  $5^4 \cdot 2b = \text{пятая степень}$ , и легко проверить, что  $a$  и  $b$  удовлетворяют тем же условиям, что  $A$  и  $B$ , а именно: в дополнение к тому, что  $5^4 \cdot 2B$  и  $A^4 + 10A^2B^2 + 5B^4$  должны быть пятыми степенями, требуется еще, чтобы  $A$  и  $B$  были взаимно простыми различной четности и чтобы  $A$  не делилось ни на 2, ни на 5. Следовательно, рассуждение может повторяться без конца, а это приводит к невозможному бесконечному спуску, а именно к последовательности *положительных* чисел  $B$ , которые убывают в силу соотношения  $2B^2 = D = b(5a^4 + 50a^2b^2 + 25b^4)$ , ибо оно дает  $b > 0$  и  $2B^2 > 25b^4$ ,  $B > b$ . Таким образом, чтобы доказать, что рассматриваемый случай невозможен, достаточно доказать импликацию

$$P^2 - 5Q^2 = \text{пятая степень} \Rightarrow P + Q\sqrt{5} = (A + B\sqrt{5})^5$$

в тех случаях, в которых она выше использовалась.

Как замечает Дирихле в начале своей работы, имеются и другие способы представить число  $P^2 - 5Q^2$  в виде пятой степени. В самом деле, решение уравнения Пелля  $9^2 - 5 \cdot 4^2 = 1$  показывает, что если  $P$  и  $Q$  определены равенством  $P + Q\sqrt{5} = (A + B\sqrt{5})^5 (9 + 4\sqrt{5})^k$  при произвольно выбранных  $A, B, k$ , то  $P^2 - 5Q^2 = (P + Q\sqrt{5})(P - Q\sqrt{5}) = (A^2 - 5B^2)^5$ . Значит, приведенная выше импликация не имеет места. Идея Дирихле заключалась в том, чтобы отыскать *дополнительные условия* для  $P$  и  $Q$ , выполнение которых обеспечивало бы справедливость импликации. И он нашел очень простое условие. Заметим, что если  $P + Q\sqrt{5} = (A + B\sqrt{5})^5$ , то число  $Q = 5A^4B + 50A^2B^3 + 25B^5$  должно делиться на 5. Таким образом,  $5 \mid Q$  — необходимое условие для справедливости импликации. Дирихле доказал, что в случае, когда  $P$  и  $Q$  взаимно просты и имеют различную четность, это условие также и достаточно, т. е. доказал следующую лемму.

**Лемма.** Пусть  $P$  и  $Q$  — такие взаимно простые целые числа, что  $P^2 - 5Q^2$  есть пятая степень,  $5 \mid Q$  и  $P$  и  $Q$  имеют различную четность. Тогда существуют такие целые числа  $A$  и  $B$ , что  $P + Q\sqrt{5} = (A + B\sqrt{5})^5$ .

Заметим, что в рассмотренных ранее случаях дополнительное условие  $5 \mid Q$  выполнено: в первом случае — поскольку из условия  $5^2 \cdot 2r = \text{пятая степень}$  вытекает  $5 \mid r \mid Q$ , а во втором — поскольку из условия  $5^4 \cdot 2B = \text{пятая степень}$  вытекает  $5 \mid B \mid D$ . Помимо этого в обоих случаях были выполнены и условия, что  $P$  и  $Q$  взаимно просты и имеют различную четность. Следовательно, как только лемма будет доказана, из нее будет следовать, что Последняя теорема Ферма при  $n = 5$  верна для случая, когда тот член уравнения  $x^5 + y^5 = z^5$ , который делится на 5, делится также и на 2.

Лемму можно доказать почти тем же способом, как изложенный в гл. 2, при помощи которого Эйлер нашел наиболее общее представление чисел в виде  $a^2 + b^2$ ,  $a^2 + 2b^2$ ,  $a^2 + 3b^2$ , но имеется одно существенное различие. Если попытаться применить методы Эйлера к представлениям в виде  $a^2 - 5b^2$ , то для предложения, аналогичного предложениям (4) и (5') из § 2.4, эта попытка не проходит. А именно, этим способом не удастся доказать утверждение: *если  $a$  и  $b$  взаимно просты, то каждый нечетный делитель числа  $a^2 - 5b^2$  может быть записан в виде  $p^2 - 5q^2$* . И действительно, как отмечалось в конце § 1.7, аналогичное утверждение для представлений в виде  $a^2 + 5b^2$  неверно. Однако из гауссовой теории бинарных квадратичных форм, изложенной в его *Disquisitiones Arithmeticae*, легко следует, что для представлений в виде  $a^2 - 5b^2$  это утверждение верно, хотя методы Эйлера и не



подходят для его доказательства. Этот факт оказывается простым следствием теории, приведенной в гл. 8 (см. упр. 11 к § 8.5).

После принятия этого факта на веру методы гл. 2 уже позволяют доказать, что если  $a$  и  $b$  взаимно просты и имеют различную четность, а  $a^2 - 5b^2 = P_1^{n_1} P_2^{n_2} \dots P_k^{n_k}$  — разложение на простые сомножители числа  $a^2 - 5b^2$ , то существуют такие целые  $p_i, q_i$  ( $i = 1, 2, \dots, k$ ) и  $t, u$ , что  $P_i = p_i^2 - 5q_i^2$ ,  $1 = t^2 - 5u^2$  и

$$a + b\sqrt{5} = (p_1 + q_1\sqrt{5})^{n_1} (p_2 + q_2\sqrt{5})^{n_2} \dots \dots (p_k + q_k\sqrt{5})^{n_k} (t + u\sqrt{5}).$$

Вкратце рассуждение проводится так. На основании недоказанного, но принятого на веру факта существуют такие  $p_1, q_1$ , что  $p_1^2 - 5q_1^2 = P_1$  (причем  $P_1$  нечетно, поскольку  $a$  и  $b$  разной четности). Число  $P_1$  делит как  $a^2 - 5b^2$ , так и  $p_1^2 - 5q_1^2$ , поэтому оно делит также и  $(p_1b - q_1a)(p_1b + q_1a) = p_1^2b^2 - q_1^2a^2 = p_1^2b^2 - 5q_1^2b^2 + 5q_1^2b^2 - q_1^2a^2 = b^2(p_1^2 - 5q_1^2) - q_1^2(a^2 - 5b^2)$ . Значит,  $P_1$  делит либо  $p_1b - q_1a$ , либо  $p_1b + q_1a$ , и, изменяя в случае необходимости знак коэффициента  $q_1$ , мы можем предполагать, что  $P_1$  делит  $p_1b + q_1a$ . Тогда, поскольку из равенства  $(a + b\sqrt{5})(p_1 + q_1\sqrt{5}) = (ap_1 + 5bq_1) + (aq_1 + bp_1)\sqrt{5}$  вытекает равенство  $(a^2 - 5b^2)P_1 = (ap_1 + 5bq_1)^2 - 5(aq_1 + bp_1)^2$ , целое число  $ap_1 + 5bq_1$  также делится на  $P_1$ . Пусть, например,  $(ap_1 + 5bq_1) + (aq_1 + bp_1)\sqrt{5} = P_1(c + d\sqrt{5})$ . Это дает  $(a + b\sqrt{5}) \cdot (p_1 + q_1\sqrt{5}) = P_1(c + d\sqrt{5})$ , откуда, умножая на  $p_1 - q_1\sqrt{5}$  и сокращая обе части равенства на  $P_1$ , получаем  $a + b\sqrt{5} = (p_1 - q_1\sqrt{5})(c + d\sqrt{5})$ . Так как  $a^2 - 5b^2 = (p_1^2 - 5q_1^2)(c^2 - 5d^2)$ , отсюда следует, что  $c^2 - 5d^2 = (a^2 - 5b^2)/P_1$ , и один из простых делителей числа  $a^2 - 5b^2$  исключен.

Затем процесс можно повторять до тех пор, пока не окажутся исключенными все простые делители, в результате чего число  $a + b\sqrt{5}$  запишется как произведение сомножителей вида  $p + q\sqrt{5}$ , количество которых в этом произведении равно  $n_1 + n_2 + \dots + n_k + 1$ , по одному на каждый простой делитель числа  $a^2 - 5b^2$  и один, для которого  $p^2 - 5q^2 = 1$ . Более того, если один и тот же простой делитель  $P$  встречается дважды, то в обоих случаях можно использовать одно и то же представление  $P = p^2 - 5q^2$  и исключаемый делитель  $p \pm q\sqrt{5}$  будет одним и тем же с точностью разве лишь до знака коэффициента  $q$ . Однако и этот знак обязан быть одним и тем же, ибо, если бы встретились оба делителя  $p + q\sqrt{5}$  и  $p - q\sqrt{5}$ , это привело бы к равенству  $a + b\sqrt{5} = (p^2 - 5q^2)(C + D\sqrt{5})$ , которое противоречило бы предположению о взаимной простоте  $a$  и  $b$ .

Таким образом, если  $P, Q$  взаимно просты и разной четности, а  $P^2 - 5Q^2$  является пятой степенью, то

$$P + Q\sqrt{5} = (A + B\sqrt{5})^5 (t + u\sqrt{5}),$$

где  $t^2 - 5u^2 = 1$ . Для доказательства леммы достаточно показать, что если  $Q$  делится на 5, то  $t + u\sqrt{5}$  можно свести к  $1 + 0\sqrt{5}$ . Это естественным путем приводит к исследованию возможных решений уравнения  $t^2 - 5u^2 = 1$ , т. е. решений уравнения Пелля в случае  $A = 5$ . Так как  $(9 + 4\sqrt{5})(9 - 4\sqrt{5}) = 1$ , то ясно, что равенство  $\pm(9 + 4\sqrt{5})^k = t + u\sqrt{5}$  дает решение для каждого целого  $k$ , положительного, отрицательного или равного нулю. Обратно, намеченные в упражнениях к § 1.9 соображения показывают, что такой вид имеют *все* решения. (Этот факт будет вновь доказан в гл. 8. См., например, упр. 2 к § 8.4.) Так как каждое целое  $k$  может быть записано в виде  $5q + r$ , где  $r = 0, 1, 2, 3$  или 4, то  $P + Q\sqrt{5} = (A + B\sqrt{5})^5 (9 + 4\sqrt{5})^r$ , где  $0 \leq r \leq 4$ . Значит, достаточно показать, что если  $Q \equiv 0 \pmod{5}$ , то  $r$  не может быть равно 1, 2, 3, 4. Пусть  $C + D\sqrt{5} = (A + B\sqrt{5})^5$  и  $E + F\sqrt{5} = (9 + 4\sqrt{5})^r$ . Тогда  $D \equiv 0 \pmod{5}$ , и из  $Q = CF + DE \equiv 0 \pmod{5}$  следует, что  $CF \equiv 0 \pmod{5}$ . Но  $C \not\equiv 0 \pmod{5}$ , поскольку из  $C \equiv 0 \pmod{5}$  вытекало бы, что  $P$  и  $Q$  оба делятся на 5. Значит,  $F \equiv 0 \pmod{5}$ . Но если бы имело место  $r \geq 1$ , то по формуле бинома число  $F$  равнялось бы слагаемому  $r \cdot 9^{r-1} \cdot 4$  плюс члены, делящиеся на 5, и  $F$  не могло бы делиться на 5; значит, из  $F \equiv 0 \pmod{5}$  вытекает  $r = 0$ , что и требовалось доказать. Этим завершается предложенное Дирихле доказательство невозможности *первого случая*.

Первое полное доказательство Последней теоремы Ферма для пятых степеней было опубликовано вскоре после этого, в сентябре 1825 г., Лежандром в его втором дополнении к *Théorie des Nombres*. Доказательство Лежандра первого случая, по существу, ничем не отличается от доказательства Дирихле, что Лежандр и признает в подстрочном примечании <sup>1)</sup>, где он пишет: «Анализ, подобный только что проведенному, позволяет доказать неразрешимость уравнения  $x^5 + y^5 = Az^5$  для довольно большого числа значений  $A$ ; это и было сделано г-ном Lejeune Dieterich [sic!] в заметке, которая была недавно представлена в Академию и получила там одобрение». Затем Лежандр переходит к доказательству того, что *второй случай* также невозможен, т. е. к тому, что оказалось не под силу Дирихле, как он сам это признавал в июле.

<sup>1)</sup> Второе дополнение было также опубликовано в виде заметки [L7] в Трудах Академии, и эта публикация почему-то датирована 1823 г. (см. Диксон [D2], т. 2, стр. 734), но это примечание показывает, что заметка вышла *после* июля 1825 г.

Это убедительный контрпример к общепринятому мнению, будто в математике только молодые люди могут сделать что-то важное.

Предложенное Лежандром доказательство второго случая не было естественным и включало в себя большое количество искусственных приемов, что, по-видимому, отражало почтенный возраст и многолетний опыт Лежандра. Спустя еще несколько месяцев, в ноябре 1825 г., Дирихле представил добавление к своей июльской статье, в котором он доказал второй случай другим способом, служащим более естественным продолжением доказательства первого случая. Это доказательство, по существу, и приводится ниже.

Во втором случае уравнение  $x^5 + y^5 = z^5$  можно привести к виду

$$u^5 \pm v^5 = w^5,$$

где  $u$ ,  $v$  и  $w$  — попарно взаимно простые положительные целые числа, причем  $w$  делится на 5, а  $u$  и  $v$  имеют разную четность. Пусть  $p = u + v$  и  $q = u - v$ . Тогда

$$u^5 \pm v^5 = \left( \frac{p+q}{2} \right)^5 \pm \left( \frac{p-q}{2} \right)^5,$$

и, меняя местами  $p$  и  $q$ , как и раньше, если понадобится, мы получаем

$$\begin{aligned} 2^{-5} \cdot 2 (p^5 + 10p^3q^2 + 5pq^4) &= w^5, \\ p (p^4 + 10p^2q^2 + 5q^4) &= 2^4 w^5. \end{aligned}$$

Как и раньше,  $p$  делится на 5, скажем  $p = 5r$ , а  $q$  не делится. Таким образом,

$$5^2 r (q^4 + 50r^2 q^2 + 125r^4) = 2^4 w^5.$$

Сомножители  $5^2 r$  и  $q^4 + 50r^2 q^2 + 125r^4$  взаимно просты, и первый из них нечетен ( $p$  и  $q$  оба нечетны), поэтому

$$\begin{aligned} 5^2 r &= \text{пятая степень}, \\ (q^2 + 25r^2)^2 - 5 (10r^2)^2 &= 2^4 \cdot (\text{пятая степень}). \end{aligned}$$

Квадрат любого нечетного числа есть 1 по модулю 8, значит, число  $q^2 + 25r^2$  равно 2 по модулю 8, а поэтому оно делится на 2, но не делится на  $2^2$ . Следовательно, второе равенство можно записать в виде

$$\left( \frac{P}{2} \right)^2 - 5 \left( \frac{Q}{2} \right)^2 = \text{пятая степень},$$

где  $P$  и  $Q$  — нечетные числа, равные соответственно  $(q^2 + 25r^2)/2$  и  $5r^2$ . Заметим, что  $Q$  делится на 5. Ниже мы покажем, что в этой ситуации найдутся такие нечетные числа  $A$  и  $B$ , что

$$\frac{P}{2} + \frac{Q}{2} \sqrt{5} = \left( \frac{A}{2} + \frac{B}{2} \sqrt{5} \right)^5.$$

Отсюда следует, что

$$\frac{Q}{2} = 5 \frac{A^4 B}{2^5} + 10 \frac{A^2 B^3}{2^5} 5 + \frac{B^5}{2^5} 5^2,$$

и, поскольку  $5^2 r$  — пятая степень, мы заключаем, что число

$$(5^2 r)^2 = 5^3 Q = 5^4 B \left[ \frac{A^4}{2^4} + 10 \frac{A^2 B^2}{2^4} + 5 \frac{B^4}{2^4} \right]$$

является пятой степенью, а значит,

$$5^4 B [A^4 + 10A^2 B^2 + 5B^4] = 2^4 \cdot (\text{пятая степень}).$$

Но  $A$  и  $B$  взаимно просты (они оба нечетны и любой их общий простой делитель делил бы как  $P$ , так и  $Q$ ) и  $A$  не делится на 5 (иначе  $P$  делилось бы на 5, откуда следовало бы, что и  $q$  делится на 5), а поэтому, как обычно,

$$5^4 B = \text{пятая степень},$$

$$A^4 + 10A^2 B^2 + 5B^4 = 2^4 \cdot (\text{пятая степень}).$$

Первое из этих равенств показывает, что  $5 \mid B$ , а второе можно переписать в виде

$$\left( \frac{A^2 + 5B^2}{2^2} \right)^2 - 5 \left( \frac{B^2}{2} \right)^2 = \text{пятая степень}.$$

Но  $A^2 + 5B^2 \equiv 6 \pmod{8}$ , так что это равенство имеет вид

$$\left( \frac{p}{2} \right)^2 - 5 \left( \frac{q}{2} \right)^2 = \text{пятая степень},$$

где  $p$  и  $q$  — такие взаимно простые нечетные числа, что  $5 \mid q$ . Далее, лемма, которую предстоит доказать, дает

$$\frac{p}{2} + \frac{q}{2} \sqrt{5} = \left( \frac{a}{2} + \frac{b}{2} \sqrt{5} \right)^5,$$

и посредством такой же последовательности шагов мы получаем

$$a^4 + 10a^2 b^2 + 5b^4 = 2^4 \cdot (\text{пятая степень}).$$

Это дает бесконечно убывающую (см. упр. 1) последовательность положительных пятых степеней, а следовательно, приводит к противоречию.

Таким образом, остается лишь доказать, что если  $P$  и  $Q$  — такие взаимно простые нечетные числа, что

$$\left( \frac{P}{2} \right)^2 - 5 \left( \frac{Q}{2} \right)^2 = \text{пятая степень}$$

(заметим, что  $P^2 - 5Q^2 \equiv 4 \pmod{8}$ , и поэтому число  $(P/2)^2 - 5(Q/2)^2$  обязано быть нечетным целым) и если  $Q$  делится на 5,

то существуют такие нечетные числа  $A$  и  $B$ , что

$$\frac{P}{2} + \frac{Q}{2} \sqrt{5} = \left( \frac{A}{2} + \frac{B}{2} \sqrt{5} \right)^5.$$

Это можно доказать следующим образом. По модулю 4 либо  $P \equiv Q$ , либо  $P \equiv -Q$ . В первом из этих случаев число  $[(P/2) + (Q \sqrt{5}/2)] \cdot [(3/2) + (\sqrt{5}/2)] = ((3P + 5Q)/4) + ((P + 3Q) \sqrt{5}/4)$  имеет вид  $C + D \sqrt{5}$ , где  $C$  и  $D$  — целые, а во втором  $[(P/2) + (Q \sqrt{5}/2)] [(3/2) - (\sqrt{5}/2)] = C + D \sqrt{5}$ , где  $C$  и  $D$  — целые. Тогда равенство

$$\begin{aligned} \left( \frac{P}{2} \right)^2 - 5 \left( \frac{Q}{2} \right)^2 &= \left( \frac{P}{2} + \frac{Q}{2} \sqrt{5} \right) \left( \frac{P}{2} - \frac{Q}{2} \sqrt{5} \right) = \\ &= (C + D \sqrt{5}) \left( \frac{3}{2} \pm \frac{1}{2} \sqrt{5} \right) (C - D \sqrt{5}) \left( \frac{3}{2} \mp \frac{1}{2} \sqrt{5} \right) = C^2 - 5D^2 \end{aligned}$$

показывает, что  $C^2 - 5D^2$  является нечетной пятой степенью, а равенство  $(P/2) + (Q \sqrt{5}/2) = [C + D \sqrt{5}] [(3/2) \mp (\sqrt{5}/2)]$  показывает, что  $C$  и  $D$  взаимно просты. Следовательно, как было показано выше,  $C + D \sqrt{5} = (c + d \sqrt{5})^5 (9 + 4 \sqrt{5})^k$ , где  $k$  равно 0, 1, 2, 3 или 4. Простой подсчет дает  $((3/2) + (\sqrt{5}/2))^3 = 9 + 4 \sqrt{5}$ , так что

$$\frac{P}{2} + \frac{Q}{2} \sqrt{5} = (c + d \sqrt{5})^5 \left( \frac{3}{2} + \frac{1}{2} \sqrt{5} \right)^{3k} \left( \frac{3}{2} + \frac{1}{2} \sqrt{5} \right)^{\pm 1},$$

и остается лишь показать, что если  $Q$  делится на 5, то из десяти возможных значений — 1, 1, 2, 4, 5, 7, 8, 10, 11, 13 показателя  $3k \pm 1$  могут встретиться только 5 и 10. Пусть  $m = 3k \pm 1$ ,  $(\alpha/2) + (\beta \sqrt{5}/2) = ((3/2) + (\sqrt{5}/2))^m$  и  $\gamma + \delta \sqrt{5} = (c + d \sqrt{5})^5$ . Тогда  $\delta$  делится на 5, а  $\gamma$  не делится. Значит, из  $Q = \gamma\beta + \alpha\delta \equiv 0 \pmod{5}$  следует  $\beta \equiv 0 \pmod{5}$ . Но по формуле бинома

$$\frac{\beta}{2} = m \left( \frac{3}{2} \right)^{m-1} \left( \frac{1}{2} \right) + \text{члены, содержащие } 5,$$

$$2^{m-1}\beta = m \cdot 3^{m-1} + \text{члены, содержащие } 5,$$

а это показывает, что из  $\beta \equiv 0 \pmod{5}$  следует  $m \equiv 0 \pmod{5}$ . Этим завершается доказательство (кроме доказательства того, что если  $A$  и  $B$  взаимно просты, то все нечетные простые делители числа  $A^2 - 5B^2$  сами имеют вид  $p^2 - 5q^2$ ).

## Упражнения

1. Покажите, что невозможно найти такие взаимно простые нечетные числа  $A$  и  $B$ , чтобы  $5^4 B$  было пятой степенью, а  $A^4 + 10A^2 B^2 + 5B^4$  было пятой степенью, умноженной на  $2^4$ . [В тексте уже все сделано, кроме доказательства того, что последовательность пятых степеней действительно убывает.]

2. Покажите, что для доказательства того, что все нечетные делители числа  $A^2 - 5B^2$  ( $A, B$  взаимно просты) сами имеют вид  $p^2 - 5q^2$ , достаточно доказать это для случая нечетных *простых* делителей.

### 3.4. Случаи $n = 14$ и $n = 7$

При любых попытках доказать Последнюю теорему Ферма элементарными средствами — скажем, не прибегая к методам куммеровской теории идеальных простых делителей, — нужно принимать во внимание тот факт, что даже один только частный случай  $n = 7$  в течение многих лет не поддавался усилиям лучших европейских математиков. Конечно, вполне возможно, что они подходили к проблеме ложными путями и что существует какая-то простая идея — возможно, открытая Ферма, — применимая ко всем случаям; однако, с другой стороны, более вероятно, что идея, пригодная для *любых*  $n$ , была бы найдена, хотя бы в неуклюжей форме, при интенсивном поиске для *одного*  $n$ .

В 1832 г., через семь лет после того, как Дирихле и Лежандр доказали случай  $n = 5$ , Дирихле опубликовал [D5] доказательство случая  $n = 14$ . Конечно, это слабее случая  $n = 7$  (каждая 14-я степень является 7-й степенью, но не наоборот), и такая публикация была своего рода признанием неудачи со случаем  $n = 7$ . Прошло еще семь лет, прежде чем в 1839 г. Ламе опубликовал первое доказательство случая  $n = 7$ . Эти доказательства довольно длинные и носят технический характер, а так как они были перекрыты доказательством Куммера Последней теоремы Ферма для целого класса показателей, который содержит 7, то заниматься ими здесь нет нужды. Их стоит упомянуть лишь постольку, поскольку они бросают свет на технические приемы, которые были испробованы и привели лишь к частичному успеху, и поскольку они дают некоторое представление о путях, возможно приведших Куммера к его открытиям.

Доказательство Дирихле для случая  $n = 14$  опирается в сущности на ту же технику, что и доказательство для  $n = 5$ , которое в свою очередь следует рассуждению Эйлера в случае  $n = 3$ ; при этом, конечно, проявляется большая изобретательность в вычислениях. Уже не удивительно, что оно опирается на лемму, согласно которой если  $A^2 + 7B^2$  является 14-й степенью и  $7 \mid B$ , то  $A + B\sqrt{-7} = (a + b\sqrt{-7})^{14}$  для некоторых целых  $a$  и  $b$ . Эта лемма в сочетании с вдохновенными алгебраическими манипуляциями и обычным рассуждением бесконечного спуска и дает доказательство. (Подробнее см. упр. 1.)

Доказательство Ламе является в некотором роде оправданием неудачи Дирихле со случаем  $n = 7$ , поскольку Ламе обнаружил, что для решения этой проблемы необходимо ввести какую-то совершенно новую технику. Его рассуждения трудны, немотиви-



рованы и, хуже всего, кажутся безнадежно привязанными к случаю  $n = 7$ . Здесь мы не будем приводить никакого описания или краткого изложения этого доказательства<sup>1)</sup> (очень краткое изложение см. у Диксона [D2], т. 2, стр. 737). Кажется, будто это доказательство ведет к опушке непроходимой чащи; приступать с подобными средствами к следующему случаю,  $n = 11$ , представлялось совершенно безнадежной затеей, и стала неизбежной переоценка методов. В течение последующих восьми лет, до 1847 г., ничего достопримечательного о случаях  $n > 7$  ( $n$  — простое) опубликовано не было, а грандиозный прогресс 1847 г. был основан на принципах, никак не связанных с доказательством Ламе для  $n = 7$ . Скорее они связаны с принципами доказательств для  $n = 3$  и  $n = 5$ , но основаны на совсем другой их интерпретации. А именно, на интерпретации не в терминах квадратичных форм  $x^2 + 3y^2$  и  $x^2 - 5y^2$ , а в терминах форм  $n$ -й степени  $x^n + y^n$  (т. е.  $x^3 + y^3$  и  $x^5 + y^5$ ). Как будет видно в следующем параграфе, Ламе сам оказался вдохновителем, если не создателем, этой новой интерпретации.

## Упражнения

1. Вот набросок доказательств Дирихле. Восполните детали. Пусть  $x^{14} + y^{14} = z^{14}$ . Можно считать, что  $x, y, z$  попарно взаимно просты и положительны;  $z$  не делится на 7, поскольку сравнение  $a^2 + b^2 \equiv 0 \pmod{7}$  невозможно. Значит, можно предположить, что  $z^{14} - x^{14} = y^{14}$ , где  $y$  делится на 7. Перепишем  $z^{14} - x^{14}$  в виде  $a(a^6 + 7b^2)$ , где  $a = z^2 - x^2$ ,  $b = zx$  ( $z^4 - z^2x^2 + x^4$ ). Числа  $a, b$  взаимно просты и разной четности. Из  $a = 7c$ ,  $7 \nmid b$ , так что  $7^2c(b^2 + 7(7^2c^3)^2) = y^{14}$ , вытекает, что  $7^2c$  и  $b^2 + 7(7^2c^3)^2$  являются 14-ми степенями. Предположите известным (см. § 8.5), что нечетный простой делитель числа вида  $x^2 + 7y^2$ , где  $x$  и  $y$  взаимно просты, должен сам иметь такой вид, и установите, что  $b + 7^2c^3 \sqrt{-7} = (d + e \sqrt{-7})^{14}$ . Далее, выражение  $2 \cdot 7^2c^3 \sqrt{-7} = (d + e \sqrt{-7})^{14} - (d - e \sqrt{-7})^{14}$  можно переписать так, как это раньше делалось с  $z^{14} - x^{14}$ , с тем чтобы найти выражение  $7^2c^3 = 2 \cdot de [2^{12} (-7)^3 d^6 e^6 + 7f^2]$ , где  $f = (d^2 + 7e^2)(d^4 - 98d^2e^2 + 49e^4)$ . Числа  $d, e$  имеют разную четность и взаимно просты. Число  $f$  не делится на 2 и 7, а  $d, e, f$  взаимно просты. Выражение  $7^2c^3 = 2 \cdot 7 \cdot de [f^2 - (2^6 \cdot 7d^3e^3)^2]$  разлагается в произведение трех попарно взаимно простых сомножителей  $2 \cdot 7 \cdot de$ ,  $f \pm 2^6 \cdot 7d^3e^3$ . Вспомните, что  $7^2c$  есть 14-я степень, и заключите на этом основании, что  $2 \cdot 7^5de$ ,  $f + 2^6 \cdot 7d^3e^3$ ,  $f - 2^6 \cdot 7d^3e^3$  все являются 14-ми степенями. Итак,  $2^7 \cdot 7d^3e^3$  является, с одной стороны, разностью 14-х степеней, а с другой стороны, произведением  $2^4$  на 14-ю степень. Короче говоря, найдено решение уравнения  $Z^{14} - X^{14} = 2^4 Y^{14}$ . Кроме того,  $X, Y, Z$  попарно взаимно просты и  $Y$  делится на 7. Повторите всю процедуру, чтобы найти решение уравнения  $\mathcal{X}^{14} - \mathcal{X}^{14} = 2^{12} \mathcal{Y}^{14}$ , где  $\mathcal{Y}$  делится на 7. Более общо, равенство  $z^{14} - x^{14} = 2^k y^{14}$  ( $k \geq 0$ ), где  $x, y, z$  попарно взаимно просты и  $y$  делится на 7, приводит к равенству  $Z^{14} - X^{14} = 2^{4+9k} Y^{14}$ , где  $Y$  делится на 7. Кроме того,  $Z$  намного меньше, чем  $z$ . Следовательно, равенство  $z^{14} - x^{14} = 2^k y^{14}$  ( $k \geq 0$ ,  $7 \mid y$ ) невозможно из-за бесконечного спуска.

<sup>1)</sup> Должен чистосердечно признаться, что я не разобрался в нем до конца.

# КУММЕРОВА ТЕОРИЯ ИДЕАЛЬНЫХ ДЕЛИТЕЛЕЙ

## 4.1. События 1847 года

Сообщения Парижской Академии и Прусской Академии в Берлине за 1847 г. рассказывают о драматическом эпизоде в истории Последней теоремы Ферма. Эпизод начинается докладом, сделанным 1 марта на собрании Парижской Академии ([A1], стр. 310), в котором Ламе объявил, испытывая, вероятно, сильное волнение, что он нашел доказательство невозможности равенства  $x^n + y^n = z^n$  для  $n > 2$  и, следовательно, полностью решил эту давнюю знаменитую проблему. Краткий набросок доказательства, который дал Ламе, был, как он несомненно осознал позже, увы, недостаточным, и нет необходимости рассматривать его здесь в подробностях. Однако его основная идея была простой и убедительной и оказалась центральной в последующем развитии теории. Доказательства случаев  $n = 3, 4, 5, 7$ , которые были найдены к тому времени, все опирались на такие алгебраические разложения, как  $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$  в случае  $n = 3$ . Ламе ощущал, что все большие затруднения при переходе к большим  $n$  вызываются ростом степени одного из сомножителей в этом разложении, и высказал мысль, что их можно преодолеть, *полностью* разложив выражение  $x^n + y^n$  на  $n$  линейных сомножителей. Это можно сделать посредством введения такого *комплексного* числа  $r$ , что  $r^n = 1$ , и использования алгебраического тождества

$$x^n + y^n = (x + y)(x + ry)(x + r^2y) \dots (x + r^{n-1}y) \quad (n \text{ нечетно}). \quad (1)$$

(Например, если  $r = \cos(2\pi/n) + i \sin(2\pi/n) = e^{2\pi i/n}$ , то полином  $X^n - 1$  имеет  $n$  различных корней  $1, r, r^2, \dots, r^{n-1}$ , и на основании элементарных алгебраических соображений мы имеем:  $X^n - 1 = (X - 1)(X - r)(X - r^2) \dots (X - r^{n-1})$ ; полагая  $X = -x/y$  и умножая на  $-y^n$ , получаем искомое тождество (1). Если говорить очень коротко, то идея Ламе состоит в применении технических приемов, использовавшихся ранее для элементарного, неполного разложения выражения  $x^n + y^n$  (в частных случаях), к его полному разложению. Именно, он собирался показать, что если  $x$  и  $y$  таковы, что сомножители  $x + y, x + ry, \dots, x + r^{n-1}y$  попарно взаимно просты, то равенство  $x^n + y^n = z^n$  обязывает каждый сомножитель  $x + y, x + ry, \dots$  быть

$n$ -й степенью, и извлечь отсюда невозможный бесконечный спуск. Если же  $x + y$ ,  $x + ry$ ,  $\dots$  не взаимно просты, то он собирался показать, что они имеют такой общий для них *всех* множитель  $m$ , что числа  $(x + y)/m$ ,  $(x + ry)/m$ ,  $\dots$ ,  $(x + r^{n-1}y)/m$  уже взаимно просты, а затем и к этому случаю применить сходный прием.

Ни на минуту не сомневаясь в том, что идея такого привлечения комплексных чисел — это ключ, который мог бы отпереть дверь к Последней теореме Ферма, Ламе восторженно сказал, что он не может отнести этот успех целиком на свой счет, поскольку идея была ему подсказана его коллегой Лиувиллем в случайном разговоре за несколько месяцев до этого. Однако Лиувилль со своей стороны не разделял энтузиазма Ламе. Он взял слово после выступления Ламе лишь затем, чтобы высказать некоторые сомнения относительно предложенного доказательства. Он отказывался признать какой бы то ни было свой приоритет в идее введения комплексных чисел, указывая, что многие другие математики, и среди них Эйлер, Лагранж <sup>1)</sup>, Гаусс, Коши и «более всех Якоби», использовали в прошлом комплексные числа сходным образом. Сказанное им практически сводилось к тому, что замысел Ламе входит в число первых идей, которые пришли бы в голову компетентному математику, впервые соприкоснувшись с этой проблемой. Более того, он отметил, что предложенное Ламе доказательство содержит весьма важный, по его мнению, пробел. Прав ли Ламе, спрашивал он, утверждая, что каждый сомножитель является  $n$ -й степенью, если он доказал лишь, что сомножители взаимно просты и что их произведение есть  $n$ -я степень? Конечно, в случае обычных целых чисел это утверждение было бы справедливо, но доказательство опирается <sup>2)</sup> на разложение целых чисел на простые сомножители, и никоим образом не ясно, что необходимые технические средства применимы к тем комплексным числам, для которых эти средства были нужны Ламе. Лиувилль чувствовал, что никакой восторг не оправдан, если (или пока) этот трудный вопрос не решен.

Коши, выступивший после Лиувилля, казалось, поверил в то, что Ламе, возможно, добьется успеха, поскольку он поторопился напомнить, что им самим в октябре 1846 г. на заседании Академии

---

<sup>1)</sup> Лиувилль не говорил об этом и мог этого не знать, но Лагранж действительно *явно* упоминал разложение  $(x + y)(x + ry) \dots (x + r^{n-1}y) = x^n + y^n$  в связи с Последней теоремой Ферма [L3].

<sup>2)</sup> Тот факт, что Лиувилль сразу заметил этот пробел и тотчас же увидел, что он связан с проблемой доказательства *однозначности разложения на простые сомножители* тех комплексных чисел, о которых идет речь, указывает, как мне кажется, на то, что Лиувилль, а возможно, и другие математики того времени хорошо знали о недостатках рассуждения на эту тему в «Алгебре» Эйлера (см. § 2.3). Тем не менее я не знаю ни одного автора того или более раннего периода, который бы критиковал доводы Эйлера.

была высказана идея, могущая, как он считал, привести к доказательству Последней теоремы Ферма, но ему не хватило времени для ее дальнейшего развития.

Сообщения о собраниях последующих недель свидетельствуют о большой активности со стороны Коши и Ламе в попытках осуществления своих идей. Ламе признавал логическую законность критики Лиувилля, но ни в коей мере не разделял его сомнений относительно правильности окончательного результата. Он утверждал, что его «леммы» дают способ разложения рассматриваемых комплексных чисел на множители и что все изученные им примеры подтверждают единственность разложения на простые множители. Он был уверен, что «не может быть непреодолимого препятствия между таким полным подтверждением и строгим доказательством».

На собрании 15 марта Ванцель заявил, что он *доказал* единственность разложения на простые, но его доводы покрывали только легко проверяемые случаи  $n \leq 4$  ( $n = 2$  есть случай обычных целых чисел,  $n = 3$  по существу представляет собой случай, исследованный в § 2.5, а случай  $n = 4$  был наскоро доказан Гауссом в его классической статье о биквадратичных вычетах); относительно остальных случаев он просто сказал, что, «как легко видеть», те же рассуждения применимы при  $n > 4$ . Однако это не так, и Коши сообщил об этом 22 марта. Начиная с этого времени Коши пускается в длинную серию статей, в которых он сам пытается обосновать алгоритм деления для рассматриваемых комплексных чисел — «радикальных полиномов», как он их называет, — из которого он мог бы заключить, что единственность разложения имеет место.

В сообщениях от 22 марта зарегистрировано, что Коши и Ламе *оба* депонировали в Академию «секретные пакеты». Депонирование секретных пакетов было неким установлением Академии, которое позволяло ее членам прибегать к регистрации, в качестве их собственности, некоторых идей в некоторый момент времени — не раскрывая самих этих идей — на случай, если позже возникнет дискуссия о приоритете. В свете событий марта 1847 г. почти нет сомнений в содержании этих двух пакетов. Однако, как оказалось, никаких приоритетных споров по поводу единственности разложения и Последней теоремы Ферма не возникло.

В последующие недели Ламе и Коши оба опубликовали заметки в сообщениях Академии; эти заметки досадно неясные, неполные и неубедительные. Затем, 24 мая, Лиувилль опубликовал в сообщениях письмо Куммера из Бреслау, которое заканчивало или должно было закончить всю дискуссию. Куммер написал Лиувиллю, чтобы сообщить ему, что его сомнения относительно неявного использования Ламе единственности разложения были вполне обоснованными. Куммер не только утверждал, что единственность разложения не имеет места, он включил в свое письмо копию

статьи [К6], которую опубликовал <sup>1)</sup> тремя годами раньше и в которой продемонстрировал отсутствие единственности разложения как раз там, где Ламе утверждал, что она имеет место. Тем не менее, писал далее Куммер, теория разложения может быть «спасена» введением нового типа комплексных чисел, которые он назвал «идеальными комплексными числами»; эти его результаты были опубликованы годом раньше в сообщениях Берлинской Академии <sup>2)</sup> в форме резюме [К7], а полное изложение их появилось в Журнале Крелля [К8]. В течение долгого времени он занимался приложениями этой новой теории к Последней теореме Ферма. В письме он сообщил, что ему удалось свести ее доказательство для данного  $n$  к проверке двух условий для этого  $n$ . Относительно деталей этого приложения и его двух условий он отсылал к заметке, опубликованной им в том же месяце в сообщениях Берлинской Академии (15 апреля 1847 г.). Там он действительно приводит полностью эти два условия и говорит, что у него «есть основания полагать», что  $n = 37$  не удовлетворяет им.

Записей о реакции ученых мужей Парижа на такие потрясающие новости не сохранилось. Ламе просто замолк. Что же касается Коши, он, то ли из упрямства, то ли потому, что вложил меньше усилий в успех единственности разложения, продолжал публиковать свои неясные и неубедительные статьи в течение еще нескольких недель. В своей единственной прямой ссылке на Куммера он говорит: «То немногое, что [Лиувиллем] было сказано [о работе Куммера], убеждает меня в том, что выводы, к которым пришел г-н Куммер, по крайней мере отчасти совпадают с теми, к которым я сам пришел, продолжая свои прежние исследования. Если г-н Куммер продвинул этот вопрос на несколько шагов дальше и если он действительно преуспел в преодолении всех препятствий, я первым буду аплодировать его усилиям; больше всего мы желали бы, чтобы усилия всех друзей науки объединились для познания и распространения истины». А затем он продолжает игнорировать — вместо того, чтобы пропагандировать — работу Куммера и пускается в погоню за своими собственными идеями, изредка лишь обещая при случае связать свои утверждения с работой Куммера. Но эти обещания так и не были выполнены. К концу лета он тоже впал в молчание по поводу Последней теоремы Ферма. (Однако Коши отнюдь не был молчальником; просто

---

<sup>1)</sup> Нужно признать, однако, что Куммер избрал для ее опубликования малоизвестное место. Лиувиль перепечатал ее в своем *Журнале чистой и прикладной математики* (Journal de Mathematiques Pures et Appliquées) в 1847 г., и тогда она, должно быть, впервые дошла до широкой аудитории.

<sup>2)</sup> Эта заметка была также перепечатана в Журнале Крелля в 1847 г. (Английский перевод с большим количеством ошибок содержится в книге [S2].) Креллевская перепечатка дает неправильную дату 1845 г. первоначальной публикации; точная дата — 1846 г.



он интенсивно начал печатать поток статей по математической астрономии.) Тем самым поле битвы осталось за Куммером, за которым оно фактически и было уже в течение трех лет.

Принято думать, что Куммер пришел к своим «идеальным комплексным числам» под влиянием интереса к Последней теореме Ферма, но это убеждение безусловно ошибочно. То что Куммер для обозначения простого числа использовал букву  $\lambda$ , для записи «корня  $\lambda$ -й степени из единицы», т. е. для решения уравнения  $\alpha^\lambda = 1$ , — букву  $\alpha$ , и то, что он изучал <sup>1)</sup> разложения простых чисел  $p \equiv 1 \pmod{\lambda}$  на «комплексные числа, составленные из корней  $\lambda$ -й степени из единицы», — все это явно указывает на статью Якоби [J2], которая посвящена *высшим законам взаимности*. Мемуар Куммера 1844 г. был адресован Университетом Бреслау Кёнигсбергскому университету в честь празднования его юбилея, и этот мемуар определенно посвящался Якоби, который в течение многих лет был профессором в Кёнигсберге. Правда, Куммер в 1830-е годы занимался Последней теоремой Ферма и, по всей вероятности, осознавал, к каким последствиям для этой теоремы могла бы привести его теория разложения, однако предмет, которым интересовался Якоби, а именно, высшие законы взаимности, был для него безусловно более важным и тогда, и позднее. В то самое время, когда он положил конец попыткам доказательства, предпринятым Ламе, и предложил взамен свое собственное частичное доказательство, он относился к Последней теореме Ферма скорее как к «любопытной диковинке из теории чисел, чем к важному вопросу», а позже, когда он опубликовал свой вариант высшего закона взаимности в форме недоказанной гипотезы, он говорил о высших законах взаимности как о «главном предмете и о вершине современной теории чисел».

Часто рассказывают легенду о том, что Куммер, подобно Ламе, верил в то, что он доказал Последнюю теорему Ферма, до тех пор, пока ему не сказали — по легенде, это был Дирихле, — что его аргументация опирается на недоказанное утверждение о единственности разложения на простые. Хотя эта легенда и не находится в явном противоречии с тем фактом, что Куммера интересовали прежде всего высшие законы взаимности, имеются другие причины усомниться в ее достоверности. Впервые она появилась в лекции памяти Куммера, прочитанной Гензелем в 1910 г., и хотя Гензель аттестовал свои источники как достоверные и назвал их имена, все же не стоит забывать, что легенда пересказывалась из третьих рук и через 65 лет после событий, о которых в ней говорилось. Кроме того, лицо, рассказавшее ее Гензелю, по-видимому, не было математиком, и легко вообразить,

<sup>1)</sup> Мемуар 1844 г. касался разложения только таких  $p$ . Общая проблема разложения охватывалась последующими работами 1846 и 1847 гг.



как из неправильно понятых фактов могла вырасти эта история. Легенда Гензеля могла бы подтвердиться, если бы нашелся «подготовленный к публикации черновик», который Куммер якобы написал и отправил Дирихле. Но пока этого не произошло, к этой истории следует относиться с большой долей скептицизма. Сомнительно, чтобы Куммер допустил единственность разложения, и еще более сомнительно, что он сделал это неосознанно в статье, которую он собирался опубликовать <sup>1</sup>).

Эта глава целиком посвящена теории разложения комплексных чисел вида  $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-1}\alpha^{\lambda-1}$  ( $a_0, a_1, \dots, a_{\lambda-1}$  — целые), «построенных» из комплексного корня  $\alpha$  уравнения  $\alpha^\lambda = 1$ , и теории «идеальных комплексных чисел», или дивизоров, которые Куммер ввел, чтобы «спасти» единственность разложения на простые для таких чисел. Следующая глава посвящается дальнейшему развитию этой теории, и только в последнем ее параграфе мы займемся применением этой теории к Последней теореме Ферма. К этому моменту мы сможем очень просто сформулировать два условия Куммера и сможем доказать Последнюю теорему Ферма для всех простых чисел, которые им удовлетворяют. Вся эта работа была завершена Куммером к 11 апреля 1847 г., через несколько недель после 1 марта, когда Ламе сделал свое сообщение.

## 4.2. Круговые целые

В этой главе мы попытаемся показать, что Куммер, жадный до вычислений подобно всем другим великим математикам, шел к своим открытиям не при помощи абстрактных размышлений, а накапливанием опыта в проведении многочисленных конкретных вычислительных примеров. Умение хорошо считать ценится теперь не слишком высоко, и мысль о том, что вычисления могут доставлять *удовольствие*, редко высказывается вслух. Однако Гаусс когда-то сказал, что он считает излишней публикацию полной таблицы классификации бинарных квадратичных форм, «поскольку (1) кто угодно, после приобретения небольшого навыка, может легко и без большой затраты времени вычислить, если ему это понадобится, таблицу любого конкретного детерминанта... (2) поскольку такая работа имеет прелесть сама по себе, так что получаешь истинное удовольствие, потратив четверть часа на ее выполнение для самого себя, тем более что (3) слишком редко представляется случай этим заняться» <sup>2</sup>). Можно было бы назвать еще Ньютона и Римана, проводивших длинные вычисления только ради развлечения. Материал этой главы, поскольку речь идет

<sup>1</sup>) Более полное обсуждение этого вопроса см. в [E3] и [E4].

<sup>2</sup>) Цитируется по Смитсу [S3], стр. 261, из письма Шумахеру.

о более абстрактном понятии «числа», чем понятие положительного целого числа, по необходимости оказывается несколько более трудным, чем материал предыдущих глав. Тем не менее каждый, кто уделит время проведению вычислений, несомненно убедится в том, что и сами эти вычисления и теория, которую развил из них Куммер, вполне ему посылны, а может быть, он найдет, не обязательно признавая это вслух, такую деятельность даже приятной.

Куммер использует букву  $\lambda$  для обозначения простого числа и букву  $\alpha$  для обозначения «мнимого» корня уравнения  $\alpha^\lambda = 1$ , т. е. комплексного корня этого уравнения, отличного от 1. Проблема, которую он ставит, заключается в разложении на простые сомножители чисел, «построенных» (gebildeten) из  $\alpha$  повторным применением сложения, вычитания и умножения, т. е. чисел вида

$$a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-1}\alpha^{\lambda-1}, \quad (1)$$

где  $a_0, a_1, \dots, a_{\lambda-1}$  — целые. (Чтобы понизить все степени числа  $\alpha$  с показателями больше  $\lambda - 1$ , мы пользуемся равенствами  $\alpha^\lambda = 1$ ,  $\alpha^{\lambda+1} = \alpha$ ,  $\alpha^{\lambda+2} = \alpha^2$ ,  $\dots$ . Значение  $\lambda$  фиксировано на протяжении всего обсуждения.) Эти числа, которые Коши называл «радикальными полиномами», а Куммер и Якоби рассматривали как специального типа «комплексные числа», теперь называют *круговыми целыми* <sup>1)</sup> ввиду геометрической интерпретации числа  $\alpha$  как такой точки на окружности  $|z| = 1$  комплексной  $z$ -плоскости, которая производит деление окружности на  $\lambda$  равных частей, а также ввиду важной роли, которую эти комплексные числа играют в гауссовой теории деления круга. Таким образом, в современной терминологии, проблема, поставленная Куммером — а до него Якоби, — это проблема *разложимости круговых целых*.

Вычисления над круговыми целыми выполняются очевидным образом с использованием коммутативного, ассоциативного и дистрибутивного законов и равенства  $\alpha^\lambda = 1$ . Например, при  $\lambda = 5$ ,  $(\alpha + \alpha^2 + 3\alpha^4)(\alpha^2 - 2\alpha^3) = (\alpha + \alpha^2 + 3\alpha^4)\alpha^2 - (\alpha + \alpha^2 + 3\alpha^4) \times (2\alpha^3) = \alpha^3 + \alpha^4 + 3\alpha^6 - 2\alpha^4 - 2\alpha^5 - 6\alpha^7 = \alpha^3 + \alpha^4 + 3\alpha - 2\alpha^4 - 2 - 6\alpha^2 = -2 + 3\alpha - 6\alpha^2 + \alpha^3 - \alpha^4$ . Далее, так как круговые целые являются частным случаем комплексных чисел, обе части равенства можно сокращать на ненулевой общий сомножитель, т. е. если  $f(\alpha)h(\alpha) = g(\alpha)h(\alpha)$  и  $h(\alpha) \neq 0$ , то  $f(\alpha) = g(\alpha)$ .

<sup>1)</sup> Возникает некий терминологический нюанс из-за того, что должно подразумеваться некоторое значение  $\lambda$ . Сказать: «данное комплексное число является круговым целым» недостаточно, нужно еще добавить «для такого-то  $\lambda$ ». В последующем тексте предполагается, что всегда будет понятно, каково конкретное значение  $\lambda$ , и используется краткий термин «круговое целое».

Эти правила вычислений имеют несколько неожиданное следствие: *представление круговых целых в виде (1) не однозначно*. Например, из  $1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1} = \alpha^\lambda + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1} = \alpha (1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1})$  вытекает, что либо

$$1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1} = 0, \quad (2)$$

либо  $\alpha = 1$ . Так как специально потребовано, что  $\alpha \neq 1$ , то соотношение (2) есть следствие основных предположений. Но из него вытекает, что

$$a_0 + a_1\alpha + \dots + a_{\lambda-1}\alpha^{\lambda-1} = (a_0 + c) + (a_1 + c)\alpha + \dots + (a_{\lambda-1} + c)\alpha^{\lambda-1} \quad (3)$$

для любого целого  $c$ , т. е. круговое целое, записанное в виде (1), не изменится, если ко всем коэффициентам  $a_i$  добавить одно и то же целое число  $c$ . Отсюда получается (если взять  $c = -a_{\lambda-1}$ ), что каждое круговое целое может быть записано в виде (1) с  $a_{\lambda-1} = 0$ ; в практических вычислениях оказывается неудобным настаивать на приведении круговых целых к такому виду, а лучше работать с ними в форме (1), имея в виду соотношение (3).

Естественно возникает вопрос, нет ли *других* непредвиденных соотношений среди чисел вида (1). Ответ отрицателен, и именно для этого и предполагается, что  $\lambda$  — *простое*. (Если  $\lambda = 4$ , то  $\alpha = \pm i$  и  $1 + \alpha^2 = 0$  или  $\alpha = -1$  и  $1 + \alpha = 0$ . В более общем случае, если  $\lambda = jk$ , то  $0 = 1 - \alpha^\lambda = (1 - \alpha^j)(1 + \alpha^j + \alpha^{2j} + \dots + \alpha^{\lambda-j})$  и один из сомножителей должен быть нулем.) Итак, если  $a_0 + a_1\alpha + \dots + a_{\lambda-1}\alpha^{\lambda-1} = b_0 + b_1\alpha + \dots + b_{\lambda-1}\alpha^{\lambda-1}$ , то обязательно  $a_0 - b_0 = a_1 - b_1 = \dots = a_{\lambda-1} - b_{\lambda-1}$ , так что это соотношение соответствует формуле (3). Эта теорема, являющаяся, конечно, основной в изучении круговых целых, была доказана Гауссом в начале раздела, посвященного циклотомии, в его *Disquisitiones Arithmeticae*. Простое доказательство приведено в упр. 15.

Куммер пользовался обозначением  $f(\alpha)$  (или  $g(\alpha)$ ,  $\varphi(\alpha)$ ,  $F(\alpha)$  и т. д.) для круговых целых вида (1). Большое преимущество такого обозначения в том, что оно позволяет писать  $f(\alpha^2)$  для кругового целого, получаемого из  $f(\alpha)$  заменой  $\alpha$  на  $\alpha^2$ ,  $\alpha^2$  на  $\alpha^4$ ,  $\alpha^3$  на  $\alpha^6$  и т. д., и, используя равенство  $\alpha^\lambda = 1$ , приводить результат к виду (1). Для того чтобы доказать законность такой операции, нужно показать, что из  $f(\alpha) = g(\alpha)$  вытекает  $f(\alpha^2) = g(\alpha^2)$ . Это следует из замечания, что если  $f(\alpha) = g(\alpha)$ , то  $f(\alpha)$  идентично  $g(\alpha) + c(1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1})$  для некоторого целого  $c$ ; тогда  $f(\alpha^2)$  идентично  $g(\alpha^2) + c(1 + \alpha^2 + \alpha^4 + \dots + \alpha^{2\lambda-2})$ , где степени  $\alpha^j$  при  $j > \lambda$  в  $1 + \alpha^2 + \alpha^4 + \dots + \alpha^{2\lambda-2}$  нужно привести к виду  $\alpha^{j-\lambda}$ . Таким образом, утверждение, которое нужно доказать, сводится к тому, что если через  $\varphi(\alpha)$  обозначено

$1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1}$ , то  $\varphi(\alpha^2)$  идентично  $\varphi(\alpha)$ , а этот факт легко следует из того, что для каждого целого  $j$  существует точно одно такое целое  $j' \pmod{\lambda}$ , что  $2j' \equiv j \pmod{\lambda}$  (см. приложение, § А.1). Точно таким же способом оказывается, что имеют смысл все числа  $f(\alpha^3)$ ,  $f(\alpha^4)$ ,  $\dots$ ,  $f(\alpha^{\lambda-1})$ . (Однако это не относится к  $f(\alpha^\lambda)$ , поскольку, например,  $1 + \alpha = -\alpha^2 - \alpha^3 - \alpha^4$  при  $\lambda = 5$ , но  $1 + \alpha^5 \neq -\alpha^{10} - \alpha^{15} - \alpha^{20}$ , так как в левой части стоит 2, а в правой  $-3$ .) Круговые целые  $f(\alpha)$ ,  $f(\alpha^2)$ ,  $f(\alpha^3)$ ,  $\dots$ ,  $f(\alpha^{\lambda-1})$  называются *сопряженными* числа  $f(\alpha)$ . Ясно, что отношение сопряженности есть отношение эквивалентности:  $f(\alpha)$  сопряжено  $f(\alpha)$ ; если  $g(\alpha)$  сопряжено  $f(\alpha)$ , то  $f(\alpha)$  сопряжено  $g(\alpha)$ , и если  $g(\alpha)$  сопряжено  $f(\alpha)$ , а  $h(\alpha)$  сопряжено  $g(\alpha)$ , то  $h(\alpha)$  сопряжено  $f(\alpha)$  (упр. 8).

Сопряжение круговых целых можно интерпретировать иначе. Действительно, относительно  $\alpha$  предполагается только, что  $\alpha^\lambda = 1$  и  $\alpha \neq 1$ . Если  $\alpha$  — любое число с этими свойствами, то такими же являются  $\alpha^2$ ,  $\alpha^3$ ,  $\dots$ ,  $\alpha^{\lambda-2}$  (при условии, конечно, что  $\lambda$  — простое). Поэтому сопряжение можно рассматривать как операцию замены того корня уравнения  $\alpha^\lambda = 1$  ( $\alpha \neq 1$ ), через который выражены круговые целые.

Для любого кругового целого  $f(\alpha)$  Куммер обозначает через  $Nf(\alpha)$  произведение всех  $\lambda - 1$  сопряженных числа  $f(\alpha)$ :

$$Nf(\alpha) = f(\alpha) f(\alpha^2) \dots f(\alpha^{\lambda-1}).$$

Он называет это произведение *нормой* числа  $f(\alpha)$  и приписывает этот термин Дирихле. Норма  $Nf(\alpha)$  любого кругового целого оказывается действительно *целым числом*. Чтобы доказать это, достаточно заметить, что любое сопряжение  $\alpha \mapsto \alpha^j$  ( $j = 1, 2, \dots, \lambda - 1$ ) разве лишь переставляет сомножители произведения, которым определено  $Nf(\alpha)$ , и, значит, оставляет  $Nf(\alpha)$  неизменным. Таким образом,  $Nf(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \dots + b_{\lambda-1}\alpha^{\lambda-1}$  равно числу  $b_0 + b_1\alpha^j + b_2\alpha^{2j} + \dots + b_{\lambda-1}\alpha^{(\lambda-1)j}$  для  $j = 2, 3, \dots, \lambda - 1$ . Но из  $b_0 + b_j\alpha^j + \dots = b_0 + b_1\alpha^j + \dots$  следует, что  $b_j - b_1 = b_0 - b_0 = 0$ . Значит,  $b_j = b_1$  для  $j = 2, 3, \dots, \lambda - 1$  и  $Nf(\alpha) = b_0 + b_1(\alpha + \alpha^2 + \dots + \alpha^{\lambda-1}) = b_0 - b_1$  — целое число. Более того,  $Nf(\alpha)$  — *положительное* целое число, кроме случая  $f(\alpha) = 0$ ,  $Nf(\alpha) = 0$ ; в этом можно убедиться, если заметить, что  $\alpha^{\lambda-1} = \bar{\alpha}$  (где  $\bar{\alpha}$  обозначает комплексно сопряженное числа  $\alpha$ ), откуда  $\alpha^{\lambda-2} = \bar{\alpha}^2$ ,  $\dots$ ,  $f(\alpha^{\lambda-1}) = \overline{f(\alpha)}$ ,  $f(\alpha^{\lambda-2}) = \overline{f(\alpha^2)}$ ,  $\dots$  и  $Nf(\alpha)$  оказывается произведением неотрицательных вещественных чисел (в количестве  $(\lambda - 1)/2$ ), которые положительны, если только не случится, что  $f(\alpha^j) = 0$  для некоторого, а следовательно, и для всех  $j = 1, 2, \dots, \lambda - 1$  (упр. 10).

Норма, очевидно, обладает следующим свойством: если  $f(\alpha)g(\alpha) = h(\alpha)$ , то  $Nf(\alpha) \cdot Ng(\alpha) = Nh(\alpha)$ . Таким образом, разложение кругового целого числа на два круговых целых сомножителя влечет за собой разложение обычного целого числа  $Nh(\alpha)$  на два обычных целых сомножителя. Например, при  $\lambda = 7$  круговое целое  $\alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2$  имеет норму 1247 (упр. 5). Так как 1247 есть произведение точно двух простых:  $1247 = 29 \cdot 43$ , то имеются в точности две возможности разложения числа  $\alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2$ ; первая, когда один сомножитель имеет норму 1, а другой — норму 1247, и вторая, когда один сомножитель имеет норму 29, а другой — норму 43.

Круговое целое с нормой 1 называется *единицей*. Если  $f(\alpha)$  является единицей, то произведение  $f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$ , будучи умножено на  $f(\alpha)$ , дает 1; поэтому  $f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$  называется *обратным* к  $f(\alpha)$  и обозначается  $f(\alpha)^{-1}$ . Обратно, если  $f(\alpha)$  есть круговое целое, для которого имеется круговое целое  $g(\alpha)$  со свойством:  $f(\alpha)g(\alpha) = 1$ , то легко показать (упр. 14), что  $f(\alpha)$  является единицей и  $g(\alpha) = f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$ . Единица  $f(\alpha)$  является делителем *любого* кругового целого  $h(\alpha)$ , поскольку  $h(\alpha) = f(\alpha)g(\alpha)$ , где  $g(\alpha) = f(\alpha)^{-1} \cdot h(\alpha)$ . По этой причине «сомножители» нормы 1 ничего не говорят о том числе, которое разлагается, и не считаются его истинными делителями. Таким образом, в упомянутом выше примере лишь то разложение числа  $\alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2$ , при котором один сомножитель имеет норму 29, а другой — норму 43, считалось бы «разложением». Говорят, что круговое целое  $h(\alpha)$  *неразложимо*, если оно не имеет истинных разложений в указанном смысле, т. е. если любое его разложение  $h(\alpha) = f(\alpha)g(\alpha)$  тривиально: либо  $f(\alpha)$ , либо  $g(\alpha)$  — единица. Можно было бы соблазниться назвать неразложимое круговое целое  $h(\alpha)$  «простым», но имеется другое, более сильное свойство, которому должно удовлетворять круговое целое, для того чтобы оно называлось «простым». Именно, говорят, что круговое целое  $h(\alpha)$  является *простым*, если оно только тогда делит произведение  $f(\alpha)g(\alpha)$ , когда оно делит один из сомножителей. Точнее, говорят, что  $h(\alpha)$  — простое, если существуют круговые целые, которые на него не делятся (т. е.  $h(\alpha)$  не является единицей), и если произведение любых двух круговых целых, каждое из которых не делится на  $h(\alpha)$ , есть круговое целое, не делящееся на  $h(\alpha)$ . Легко видеть, что простое круговое целое неразложимо (упр. 18). Для обычных целых чисел неразложимость влечет за собой простоту («Начала» Евклида, Книга VII, предложение 24). Тот факт, что существуют круговые целые, которые неразложимы, но не просты, лежит в основе отсутствия однозначности разложения; именно поэтому и понадобилась куммерова теория идеальной факторизации.



Как упомянуто в предыдущем параграфе, Коши и другие математики потратили значительные усилия на то, чтобы найти *алгоритм деления* для круговых целых, т. е. процесс деления с остатком, подобный тому, который применял Евклид при изучении свойств делимости положительных целых чисел (см. приложение, § А.1), и тому, который применял Гаусс при изучении свойств делимости «целых» вида  $a + bi$ . Даже Куммер в своей статье 1844 г. пытался воспользоваться таким делением с остатком для круговых целых. В то же самое время Куммер показал, как воспользоваться нормой для практического деления, т. е. еще в 1844 г. указал процесс, о котором Ламе, по-видимому, ничего не знал в 1847 г.

Пусть даны два круговых целых  $f(\alpha)$ ,  $h(\alpha)$ ; определить, имеется ли такое круговое целое  $g(\alpha)$ , что  $f(\alpha)g(\alpha) = h(\alpha)$ , и если да, то найти  $g(\alpha)$ . В этом состоит задача обычного деления, и Куммер решил ее следующим образом. Если  $f(\alpha) = 0$ , то  $g(\alpha)$  существует только тогда, когда  $h(\alpha) = 0$ , и в этом случае подойдет любое  $g(\alpha)$ . Значит, достаточно рассмотреть случай  $f(\alpha) \neq 0$ . Пусть сначала число  $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-1}\alpha^{\lambda-1}$  есть обычное целое число  $a_0$ , т. е. может быть записано в таком виде, что  $a_1 = a_2 = \dots = a_{\lambda-1} = 0$ . Тогда равенство  $f(\alpha)g(\alpha) = h(\alpha)$  показывает, что все коэффициенты числа  $h(\alpha)$  кратны  $f(\alpha) = a_0 \neq 0$ . Правда, такое условие не является содержательным, поскольку оно зависит от представления числа  $h(\alpha)$  в виде (1). Однако его можно переформулировать так, что оно окажется независимым от этого представления. Это можно сделать, сказав, что если  $h(\alpha) = a_0g(\alpha)$ , то все коэффициенты числа  $h(\alpha)$  попарно сравнимы по модулю  $a_0$ . Но это необходимое условие, очевидно, является и достаточным, ибо если все коэффициенты числа  $h(\alpha) = b_0 + b_1\alpha + \dots + b_{\lambda-1}\alpha^{\lambda-1}$  сравнимы друг с другом по модулю  $a_0$ , т. е.  $b_i \equiv b_j \pmod{a_0}$ , то все коэффициенты этого же числа, записанного в виде  $h(\alpha) = (b_0 - b_{\lambda-1}) + (b_1 - b_{\lambda-1})\alpha + \dots + (b_{\lambda-2} - b_{\lambda-1})\alpha^{\lambda-2}$ , делятся на  $a_0$ , и  $h(\alpha)$  можно представить в виде  $h(\alpha) = a_0g(\alpha)$ . Это решает задачу деления в случае  $f(\alpha) = a_0$ . Понятие нормы позволяет свести общий случай задачи к этому частному случаю. Достаточно заметить, что равенство  $f(\alpha)g(\alpha) = h(\alpha)$  эквивалентно равенству  $Nf(\alpha) \cdot g(\alpha) = h(\alpha) \times \times f(\alpha^2) f(\alpha^3) \dots f(\alpha^{\lambda-1})$ ; это показывает, что  $f(\alpha)$  делит  $h(\alpha)$  тогда и только тогда, когда целое число  $Nf(\alpha)$  делит  $h(\alpha) f(\alpha^2) \times \times f(\alpha^3) \dots f(\alpha^{\lambda-1})$ , причем если это так, то частное  $g(\alpha)$  в обоих случаях одно и то же. Этот способ деления не вполне удовлетворителен, поскольку вычисление значений  $Nf(\alpha)$  и  $h(\alpha) f(\alpha^2) \times \times f(\alpha^3) \dots f(\alpha^{\lambda-1})$  может быть очень длинным, но он показывает, что вопрос о делимости действительно имеет определенный ответ, который может быть получен за конечное число шагов.



Если для данных  $f(\alpha)$ ,  $h(\alpha)$  имеется такое  $g(\alpha)$ , что  $f(\alpha)g(\alpha) = h(\alpha)$ , то говорят, что  $f(\alpha)$  *делит*  $h(\alpha)$  или  $h(\alpha)$  *делится* на  $f(\alpha)$ . Обозначение  $f(\alpha) \mid h(\alpha)$  означает « $f(\alpha)$  делит  $h(\alpha)$ », а обозначение  $f(\alpha) \nmid h(\alpha)$  означает « $f(\alpha)$  не делит  $h(\alpha)$ ». Утверждение, что  $f(\alpha)$  делит  $h(\alpha)$ , можно также записать в виде  $h(\alpha) \equiv 0 \pmod{f(\alpha)}$ . Более общо, запись  $h_1(\alpha) \equiv h_2(\alpha) \pmod{f(\alpha)}$  означает, что  $f(\alpha)$  делит  $h_1(\alpha) - h_2(\alpha)$ .

Такова в общих чертах арифметика круговых целых. Прежде чем перейти в следующем параграфе к подробному изучению их разложения, стоит, может быть, сделать паузу и обсудить подоплеку этой арифметики. Куммер неизменно ссылается на круговые целые как на «комплексные числа», и, по крайней мере на современный слух, это наводит на мысль геометрическую картину<sup>1)</sup> для них как точек «комплексной плоскости». Этот взгляд на круговые целые имеет то преимущество, что делает некоторые свойства — в первую очередь свойство  $Nf(\alpha) \geq 0$  — легко доказываемыми; однако он ничем не помогает в понимании других свойств, например свойств разложения круговых целых, которые являются главным предметом этой главы. Кронекер, который был студентом и близким сотрудником Куммера, много лет спустя предлагал (см. [K2] и [K3]) подходить к круговым целым *абстрактно* и *алгебраически* как к множеству всех выражений вида (1) со сложением, вычитанием и умножением, определенными очевидным образом, и с единственным соотношением  $1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1} = 0$ . Этот подход более в духе алгебры сегодняшнего дня, и читатель, изучавший современную алгебру, узнает в этой конструкции факторкольцо кольца полиномов от одной переменной с целыми коэффициентами по идеалу, порожденному полиномом  $1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1}$ . Главное достоинство этого подхода в том, что он выделяет алгебраические правила вычислений в арифметике круговых целых (которые легко усваиваются даже теми, кто не привык к комплексным числам) и отодвигает на задний план все другие рассуждения.

## Упражнения

1.  $2 + \alpha + 3\alpha^2 - 2\alpha^3 = -\alpha + \alpha^2 - 4\alpha^3 - 2\alpha^4$  ( $\lambda = 5$ ). Пусть  $f(\alpha)$  есть левая часть этого равенства,  $g(\alpha)$  — правая часть. Докажите, что  $f(\alpha^3) = g(\alpha^3)$ . Имеет ли место равенство  $f(\alpha^5) = g(\alpha^5)$ ?

<sup>1)</sup> Эта геометрическая картина ясно описана в п. 38 второй статьи Гаусса [G6] о биквадратичной взаимности. Интересно отметить, что в этой статье, которая предшествует статье Якоби, как последняя предшествует статье Куммера, Гаусс ясно говорит (замечание в конце п. 30), что для изучения кубических вычетов нужно было бы рассматривать комплексные числа, построенные при помощи кубического корня из единицы, а для изучения высших вычетов нужно было бы таким же способом «ввести другие мнимые величины».

2. Умножение круговых целых можно выполнять как умножение полиномов. Например, умножение  $(\alpha^4 + 7\alpha^2 + 5\alpha + 1) \cdot (2\alpha^3 + 3\alpha^2 - \alpha + 2)$  (при  $\lambda = 5$ ) можно выполнить по следующей схеме:

			1	0	7	5	1
			0	2	3	-1	2
			<hr/>				
			2	0	14	10	2
		-1	0	-7	-5	-1	
	3	0	21	15	3		
2	0	14	10	2			
<hr/>							
2	3	13	33	10	12	9	2

и найти произведение  $2\alpha^7 + 3\alpha^6 + 13\alpha^5 + 33\alpha^4 + 10\alpha^3 + 12\alpha^2 + 9\alpha + 2 = (2 + 12)\alpha^2 + (3 + 9)\alpha + (13 + 2) + 33\alpha^4 + 10\alpha^3 = -\alpha^2 - 3\alpha + 0 + + 18\alpha^4 - 5\alpha^3$ . Эффективнее пристроить к этой схеме соотношение  $\alpha^{j+\lambda} = \alpha^j$ , записывая данное умножение в виде

1	0	7	5	1				
0	2	3	-1	2				
<hr/>								
2	0	14	10	2				
0	-7	-5	-1	-1				
21	15	3	3	0				
10	2	2	0	14				
<hr/>								
33	10	14	12	15 = 18	-5	-1	-3	0.

Используйте эту схему умножения для проверки ассоциативного закона в случае произведения трех сомножителей  $(\alpha^4 + 7\alpha^2 + 5\alpha + 1) \cdot (2\alpha^3 + 3\alpha^2 - - \alpha + 2) (4\alpha^4 + 2\alpha^3 - \alpha^2 + 5)$  при  $\lambda = 5$ .

3. Покажите, что при  $\lambda = 3$  норма любого кругового целого имеет вид  $(A^2 + 3B^2)/4$ , где  $A$  и  $B$  — целые числа одинаковой четности. Докажите, что в этом случае имеется точно 6 единиц, и найдите их все.

4. Покажите, что при  $\lambda = 5$  норма любого кругового целого имеет вид  $(A^2 - 5B^2)/4$ , где  $A$  и  $B$  — целые числа одинаковой четности. [В произведении  $f(\alpha) f(\alpha^2) f(\alpha^3) f(\alpha^4)$  умножьте сначала  $f(\alpha)$  на  $f(\alpha^4)$ . Результат имеет вид  $a + b\theta_0 + c\theta_1$ , где  $\theta_0 = \alpha + \alpha^4$ ,  $\theta_1 = \alpha^2 + \alpha^3$ . Затем убедитесь, что  $f(\alpha^2) f(\alpha^3) = a + b\theta_1 + c\theta_0$  и норма имеет вид  $(b\theta_0 + c\theta_1)(b\theta_1 + c\theta_0)$ . Один из путей вычисления дает  $-(A^2 - 5B^2)/4$ , что выглядит неверным, но таким не является.] Найдите бесконечное число единиц в этом случае.

5. Пусть  $\lambda = 7$  и  $f(\alpha) = \alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2$ . В упр. 4 к § 4.4 будет использована формула  $Nf(\alpha) = 1247$ . Выведите ее. [Сначала подсчитайте  $f(\alpha) f(\alpha^2) f(\alpha^4) = a + b\theta_0 + c\theta_1$ . Проводите вычисления, как в упр. 2.]

6. Покажите, что если  $f(\alpha) = g(\alpha)$ , то  $f(1) \equiv g(1) \pmod{\lambda}$ . Выведите отсюда, что  $Nf(\alpha) \equiv 0$  или  $1 \pmod{\lambda}$  [теорема Ферма].

7. Докажите, что  $f(\alpha) + f(\alpha^2) + \dots + f(\alpha^{\lambda-1}) \equiv -f(1) \pmod{\lambda}$ . Это дает второй вариант доказательства первой части упр. 6. [Сумму  $f(1) + f(\alpha) + f(\alpha^2) + \dots + f(\alpha^{\lambda-1})$  легко записать в явном виде.]

8. Докажите, что если  $g(\alpha)$  сопряжено  $(\alpha)$ , а  $h(\alpha)$  сопряжено  $g(\alpha)$ , то  $h(\alpha)$  сопряжено  $f(\alpha)$ . [Заметим, что  $\alpha \mapsto \alpha^j$  не является сопряжением,

если  $\lambda \mid j$ .] Докажите, что если  $g(\alpha)$  сопряжено  $f(\alpha)$ , то  $f(\alpha)$  сопряжено  $g(\alpha)$ .

9. Покажите, что если  $f(\alpha) = A\alpha^j + B\alpha^k$ , то результат упр. 6 можно следующим образом усилить: за исключением тривиальных случаев, когда  $A$  и  $B$  не взаимно просты или  $j \equiv k \pmod{\lambda}$ , каждый простой делитель числа  $Nf(\alpha)$  сравним с 0 или 1  $\pmod{\lambda}$ . [ $f(\alpha)$  есть единица, умноженная на одно из сопряженных числа  $A + B\alpha$ , откуда  $(A + B)Nf(\alpha) = A^\lambda + B^\lambda$ ,  $Nf(\alpha) = A^{\lambda-1} - A^{\lambda-2}B + \dots + B^{\lambda-1}$ . Если  $1 - k + k^2 - \dots + k^{\lambda-1} \equiv \equiv 0 \pmod{p}$ , то  $k \equiv -1$  или  $k^\lambda \equiv -1 \pmod{p}$ ,  $p \equiv 1 \pmod{\lambda}$ .]

10. Покажите, что  $\alpha^{\lambda-1}$  есть комплексно сопряженное числа  $\alpha$ . [Оба они умножаются, как  $\alpha$ .] Выполните другие шаги доказательства утверждения  $Nf(\alpha) \geq 0$ , данного в тексте.

11. Пусть  $\lambda = 5$ . Тогда  $38\alpha^3 + 62\alpha^2 + 56\alpha + 29$  делится на  $3\alpha^3 + 4\alpha^2 + 7\alpha + 1$ . Найдите частное. [Используйте способ деления, объясненный в тексте, и алгоритм умножения из упр. 2.]

12. Докажите, что  $f(\alpha)$  делится на  $\alpha - 1$  тогда и только тогда, когда  $f(1) \equiv 0 \pmod{\lambda}$ . [Примените теорему о делении с остатком.] Это дает третье доказательство первой части упр. 6. Заметим, что в упр. 11 оба числа — и делимое и делитель — делятся на  $\alpha - 1$ . Выполните оба деления и тем самым упростите решение упр. 11.

13. Пусть  $\lambda = 5$ . Выберите два круговых целых и подсчитайте их произведение. Затем используйте данный в тексте способ деления для того, чтобы разделить произведение на один из сомножителей. Прodelайте то же самое для  $\lambda = 7$ .

14. Покажите, что если  $f(\alpha)$  и  $g(\alpha)$  — такие круговые целые, что  $f(\alpha)g(\alpha) = 1$ , то  $f(\alpha)$  является единицей и  $g(\alpha) = f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$ . [Проще всего доказать, что  $Nf(\alpha) = \pm 1$ , и использовать тот факт, что норма неотрицательна.]

15. Это упражнение посвящено доказательству того, что круговые целые не удовлетворяют никаким другим соотношениям, кроме указанных в тексте. Пусть  $f(\alpha) = 0$  есть соотношение такого типа, т. е.  $f(X)$  есть полином от одной переменной с целыми коэффициентами, обращающийся в нуль, когда комплексное число  $\alpha$  подставляется в него вместо переменной  $X$ . Поскольку  $\alpha^\lambda = 1$ ,  $\alpha^{\lambda+1} = \alpha$ , ..., очевидно, можно допустить, что степень полинома  $f(X)$  не превосходит  $\lambda - 1$ . Нужно доказать, что  $f(X)$  должен быть кратным полинома  $X^{\lambda-1} + X^{\lambda-2} + \dots + X + 1$ . Пусть  $h(X) = X^{\lambda-1} + X^{\lambda-2} + \dots + X + 1$ . Найдется такое целое  $a$ , что  $f(X) - a \cdot h(X)$  имеет степень, меньшую  $\lambda - 1$ , и обращается в нуль при  $X = \alpha$ . Таким образом, достаточно доказать, что если степень  $f(X)$  меньше  $\lambda - 1$  и  $f(\alpha) = 0$ , то  $f(X)$  есть полином, равный 0. Допустим, что это не так, т. е. допустим, что  $f(X) \neq 0$ ,  $f(X)$  имеет степень, меньшую  $\lambda - 1$ , и  $f(\alpha) = 0$ . Тогда  $a \cdot h(X) = q(X)f(X) + r(X)$ , где  $a$  — целое число,  $q(X)$  и  $r(X)$  — полиномы с целыми коэффициентами и  $r(X)$  имеет меньшую степень, чем  $f(X)$ . Если  $r(X) \neq 0$ , то заменим  $f(X)$  на  $r(X)$  и повторим процесс. Значит, можно допустить, что  $a \cdot h(X) = q(X) \cdot f(X)$ . Если  $a \neq \pm 1$ , то имеется такое простое  $p$ , что  $q(X)f(X) \equiv \equiv 0 \pmod{p}$ . Отсюда вытекает, что  $q(X) \equiv 0$  или  $f(X) \equiv 0 \pmod{p}$ . Следовательно, равенство  $a \cdot h(X) = q(X)f(X)$  можно сократить на  $p$ . Таким образом, можно считать, что  $h(X) = f(X) \cdot g(X)$ . Рассмотрим это соотношение по модулю  $\lambda$ . Имеем:  $h(j) \equiv 0$  для  $j \equiv 1$ , но  $h(j) \equiv 1$  для  $j \not\equiv 1 \pmod{\lambda}$ . Иными словами, по модулю  $\lambda$  полиномы  $h(X)$  и  $(X - 1)^{\lambda-1}$  принимают одинаковые значения для всех целых значений переменной  $X$ . Так как  $h(X) = (X - 1)^{\lambda-1}$  есть полином степени, меньшей  $\lambda$  (на самом деле меньшей  $\lambda - 1$ ), все значения которого при целых  $X$  равны нулю по модулю  $\lambda$ , то рассуждение с разностями, подобное примененному в § 2.4, показывает, что  $h(X) \equiv \equiv (X - 1)^{\lambda-1} \pmod{\lambda}$ . Полином  $F(X)$  делится на  $X - 1 \pmod{\lambda}$  тогда

и только тогда, когда  $F(1) \equiv 0 \pmod{\lambda}$ . Это верно либо для  $f(X)$ , либо для  $g(X)$ , но не для обоих одновременно. Следовательно, либо  $f(X)$ , либо  $g(X)$  делится на  $(X-1)^{\lambda-1} \pmod{\lambda}$ . Так как  $f(X)$  имеет степень, меньшую  $\lambda-1$ , то  $g(X)$  обязан иметь степень  $\lambda-1$ . Отсюда степень полинома  $f(X)$  равна нулю и условие  $f(\alpha) = 0$  дает  $f = 0$ , т. е. получено противоречие. Восполните детали этого доказательства.

16. Докажите чисто алгебраическими средствами, что если  $f(\alpha)h(\alpha) = g(\alpha)h(\alpha)$  и  $h(\alpha) \neq 0$ , то  $f(\alpha) = g(\alpha)$ . [Достаточно рассмотреть случай  $g(\alpha) = 0$ . Тогда  $f(\alpha)$  удовлетворяет более слабому условию, чем  $f(\alpha)$  в упр. 15, но можно провести то же самое рассуждение.] Единственное свойство круговых целых, которое не было доказано чисто алгебраическими средствами в этом параграфе, это свойство  $Nf(\alpha) \geq 0$  в упр. 10<sup>1</sup>).

17. Докажите, что отношение сравнимости  $h_1(\alpha) \equiv h_2(\alpha) \pmod{f(\alpha)}$ , определенное в тексте, обладает при фиксированном  $f(\alpha)$  свойствами отношения эквивалентности (т. е. рефлексивно [ $h(\alpha) \equiv h(\alpha)$ ], симметрично [ $h(\alpha) \equiv k(\alpha)$  влечет за собой  $k(\alpha) \equiv h(\alpha)$ ] и транзитивно [если  $h(\alpha) \equiv k(\alpha)$  и  $k(\alpha) \equiv g(\alpha)$ , то  $h(\alpha) \equiv g(\alpha)$ ]) и согласовано со сложением и умножением (т. е. из  $h_1(\alpha) \equiv h_2(\alpha)$  и  $k_1(\alpha) \equiv k_2(\alpha)$  следует, что  $h_1(\alpha) + k_1(\alpha) \equiv h_2(\alpha) + k_2(\alpha)$  и  $h_1(\alpha)k_1(\alpha) \equiv h_2(\alpha)k_2(\alpha)$ ).

18. Докажите, что простое круговое целое неразложимо.

19. Докажите, что для обычных целых чисел неразложимое целое является простым.

### 4.3. Разложение простых чисел $p \equiv 1 \pmod{\lambda}$

Естественным первым шагом в изучении разложения круговых целых является попытка найти все *простые* в этой арифметике. В соответствии с определением предыдущего параграфа мы называем круговое целое  $h(\alpha)$  *простым*, если оно не является единицей и только тогда делит произведение двух круговых целых, когда

<sup>1)</sup> Х. У. Ленстра, мл., прислал мне следующее алгебраическое доказательство того, что  $Nf(\alpha) \geq 0$ . Положим  $g(\alpha) = f(\alpha) \cdot f(\alpha^2) \dots f(\alpha^{(\lambda-1)/2})$ . Тогда  $Nf(\alpha) = g(\alpha) \prod_{j=1}^{\lambda-1} g(\alpha^j) = g(\alpha^j) g(\alpha^{\lambda-j})$  для  $j = 1, 2, \dots, \lambda-1$ , и достаточно показать, что  $\sum_{j=1}^{\lambda-1} g(\alpha^j) g(\alpha^{\lambda-j}) \geq 0$ . Это верно для всех круговых

целых  $g(\alpha) = \sum_{i=0}^{\lambda-1} a_i \alpha^i$  (а не только для тех, которые имеют вид  $f(\alpha) \dots f(\alpha^{(\lambda-1)/2})$ ), поскольку

$$\begin{aligned} \sum_{j=1}^{\lambda-1} g(\alpha^j) g(\alpha^{\lambda-j}) &= \sum_{i=0}^{\lambda-1} \sum_{k=0}^{\lambda-1} \sum_{j=1}^{\lambda-1} a_i \alpha^{ij} a_k \alpha^{k(\lambda-j)} = \\ &= \sum_{i,k} a_i a_k \sum_{j=1}^{\lambda-1} \alpha^{(i-k)j} = (\lambda-1) \sum_{i=0}^{\lambda-1} a_i^2 - \sum_{\substack{0 \leq i, k \leq \lambda-1 \\ i \neq k}} a_i a_k = \\ &= \sum_{0 \leq i < k \leq \lambda-1} (a_i - a_k)^2 \geq 0. \end{aligned}$$

оно делит один из сомножителей, т. е.  $h(\alpha) \nmid 1$  и из  $h(\alpha) \mid f(\alpha)g(\alpha)$  вытекает, что  $h(\alpha) \mid f(\alpha)$  или  $h(\alpha) \mid g(\alpha)$ . При изучении Последней теоремы Ферма мы сразу сталкиваемся с сомножителями в равенстве  $(x + y)(x + \alpha y)(x + \alpha^2 y) \dots (x + \alpha^{\lambda-1} y) = z^\lambda$ . Поэтому настоящий параграф и следующий за ним посвящены задаче разложения биномов вида  $x + \alpha^j y$  ( $x$  и  $y$  — взаимно простые целые числа,  $j = 1, 2, \dots, \lambda - 1$ ) и, в частности, задаче нахождения всех возможных простых делителей таких биномов.

(Сосредоточение внимания на разложении биномов оправдано не только тем, что биномы сразу появляются в Последней теореме Ферма, но также и тем, что, как мы увидим в этой главе, простые делители таких биномов имеют наиболее ясный вид среди всех простых в арифметике круговых целых. Кроме того, именно эти простые делители изучал Куммер в своей первоначальной работе 1844 г., посвященной разложению круговых целых. Правда, причины, побудившие его заняться этими частного вида делителями, по-видимому, не имели никакого отношения к Последней теореме Ферма и были связаны скорее с работой Якоби [J2] о высших законах взаимности.)

Мы будем действовать методом анализа, а именно, мы предположим, что простой делитель  $h(\alpha)$  бинома  $x + \alpha^j y$  известен, и из этого предположения извлечем достаточно информации, чтобы во многих случаях сделать возможным построение таких простых делителей  $h(\alpha)$ . Тот факт, что в некоторых ситуациях конструктивный метод *не дает* ожидаемый делитель, привел Куммера сначала к наблюдению, что наивное предположение о единственности разложения несостоятельно, а затем к созданию теории идеальной факторизации, которая «спасает» единственность разложения и доставляет мощный инструмент изучения арифметики круговых целых.

Итак предположим, что  $h(\alpha)$  есть простое круговое целое, которое делит бином  $x + \alpha^j y$ , где  $x$  и  $y$  — взаимно простые целые числа и  $\alpha^j \neq 1$ . Тогда  $h(\alpha)$  делит норму  $N(x + \alpha^j y)$ , которая является обычным целым числом. Целое  $N(x + \alpha^j y)$  может быть записано в виде произведения простых целых, скажем  $N(x + \alpha^j y) = p_1 p_2 \dots p_n$  (допускаются повторения), и, поскольку  $h(\alpha)$  простое, одно из этих простых целых  $p_1, p_2, \dots, p_n$  должно делиться на  $h(\alpha)$ . Пусть  $p$  — некоторое простое целое число, делящееся на  $h(\alpha)$ . Тогда  $h(\alpha)$  не делит ни одно целое  $t$ , взаимно простое с  $p$ , поскольку в этом случае  $1 = at + br$  для некоторых целых  $a$  и  $b$  и  $h(\alpha) \mid t$  влекло бы за собой  $h(\alpha) \mid 1$  вопреки предположению, что  $h(\alpha)$  не является единицей. Таким образом, *целые числа, которые делятся на  $h(\alpha)$ , суть кратные  $p$  и только они.*



Главным техническим приемом нахождения условий на  $h(\alpha)$  будет рассмотрение сравнений по модулю  $h(\alpha)$ . Точнее, будет показано, что можно определить, сравнимы ли по модулю  $h(\alpha)$  два круговых целых, даже если само  $h(\alpha)$  не известно, а известны только  $p$ ,  $x$ ,  $y$  и  $j$ . Этот факт очень помогает в анализе  $h(\alpha)$  и последующем нахождении возможных простых делителей.

Говорят, что два круговых целых  $f(\alpha)$  и  $g(\alpha)$  сравнимы по модулю третьего кругового целого  $h(\alpha)$ , и пишут  $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)}$ , если  $h(\alpha)$  делит разность  $f(\alpha) - g(\alpha)$ . Это отношение, как и сравнимость обычных целых чисел по модулю третьего целого числа, является *рефлексивным, симметричным, транзитивным* и *согласовано со сложением и умножением*. Выпишем эти условия:  $f(\alpha) \equiv f(\alpha) \pmod{h(\alpha)}$  (рефлексивность); из  $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)}$  следует  $g(\alpha) \equiv f(\alpha) \pmod{h(\alpha)}$  (симметричность); из  $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)}$  и  $g(\alpha) \equiv \varphi(\alpha) \pmod{h(\alpha)}$  следует  $f(\alpha) \equiv \varphi(\alpha) \pmod{h(\alpha)}$  (транзитивность); из  $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)}$  следует  $f(\alpha) + \varphi(\alpha) \equiv g(\alpha) + \varphi(\alpha) \pmod{h(\alpha)}$  для всех  $\varphi(\alpha)$  (согласованность со сложением) и из  $f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)}$  следует  $f(\alpha)\varphi(\alpha) \equiv g(\alpha)\varphi(\alpha) \pmod{h(\alpha)}$  для всех  $\varphi(\alpha)$  (согласованность с умножением). Все эти утверждения непосредственно следуют из определения. Короче говоря, к этим сравнениям по модулю  $h(\alpha)$  при любом круговом целом  $h(\alpha)$  могут быть применены обычные правила выкладок со сравнениями.

Если  $h(\alpha)$ ,  $x + \alpha^j y$  и  $p$  имеют определенный выше смысл, то доказанное утверждение о том, что *целые числа*, делящиеся на  $h(\alpha)$ , кратны  $p$ , можно сформулировать как утверждение о том, что для *целых чисел*  $u$  и  $v$  сравнение  $u \equiv v \pmod{h(\alpha)}$  равносильно сравнению  $u \equiv v \pmod{p}$ . Это показывает, что  $y \not\equiv 0 \pmod{p}$ , поскольку  $y \equiv 0 \pmod{p}$  вместе с  $x + \alpha^j y \equiv 0 \pmod{h(\alpha)}$  дало бы  $x \equiv 0 \pmod{h(\alpha)}$  и  $x \equiv 0 \pmod{p}$  вопреки предположению о взаимной простоте  $x$  и  $y$ . Значит, найдется такое целое  $a$ , что  $ay \equiv 1 \pmod{p}$ . Далее,  $ay \equiv 1 \pmod{h(\alpha)}$ ;  $0 \equiv a(x + \alpha^j y) \equiv ax + \alpha^j \pmod{h(\alpha)}$ ,  $\alpha^j \equiv -ax \pmod{h(\alpha)}$ . Таким образом,  $\alpha^j$  сравнимо с некоторым целым числом по модулю  $h(\alpha)$ . Так как все степени числа  $\alpha$  являются в то же время степенями любой его данной степени  $\alpha^j$ , при условии что  $\alpha^j \neq 1$ , то предыдущее показывает, что все степени числа  $\alpha$  сравнимы с целыми числами по модулю  $h(\alpha)$ . Далее, найдется такое целое  $i$ , что  $ij \equiv 1 \pmod{\lambda}$  (поскольку  $\lambda$  простое и  $j$  не делится на  $\lambda$ ), откуда следует, что  $\alpha = \alpha^{ij} \equiv (-ax)^i \pmod{h(\alpha)}$ . Пусть  $k$  обозначает целое число, сравнимое с  $(-ax)^i$  по модулю  $p$ . Тогда  $k$  зависит только от  $p$ ,  $x$ ,  $y$  и  $j$  и обладает следующим свойством: для любого кругового целого  $g(\alpha) = a_{\lambda-1}\alpha^{\lambda-1} + \dots + a_1\alpha + a_0$  целое число  $g(k)$ , полученное заменой  $\alpha$  на  $k$  в  $g(\alpha)$ , сравнимо



с этим круговым целым  $g(\alpha)$  по модулю  $h(\alpha)$ ,  $g(\alpha) \equiv g(k) \pmod{h(\alpha)}$ . Таким образом, любое круговое целое сравнимо с целым числом по модулю  $h(\alpha)$ . Так как легко узнать, сравнимы или нет два целых числа по модулю  $h(\alpha)$ , это позволяет легко узнать, сравнимы или нет два круговых целых по модулю  $h(\alpha)$ , и доказать следующую теорему.

**Теорема.** Пусть  $h(\alpha)$  — простое круговое целое, которое делит как  $x + \alpha^j y$  ( $x, y$  взаимно просты,  $\alpha^j \not\equiv 1$ ), так и  $p$  (простое целое число). Тогда имеется такое целое число  $k$ , причем его можно найти, зная только  $x, y, j, p$ , что  $\alpha \equiv k \pmod{h(\alpha)}$  и в результате

$$f(\alpha) \equiv g(\alpha) \pmod{h(\alpha)} \iff f(k) \equiv g(k) \pmod{p},$$

где  $f(k)$  и  $g(k)$  обозначают <sup>1)</sup> целые числа, получаемые из круговых целых  $f(\alpha)$  и  $g(\alpha)$  подстановкой  $\alpha = k$ .

**Доказательство.** Поскольку  $\alpha \equiv k \pmod{h(\alpha)}$  и поскольку сравнения можно складывать и перемножать,  $f(\alpha) \equiv f(k) \pmod{h(\alpha)}$ . Аналогично,  $g(\alpha) \equiv g(k) \pmod{h(\alpha)}$ . Так как  $f(k)$  и  $g(k)$  — целые числа, то сравнение  $f(k) \equiv g(k) \pmod{h(\alpha)}$  равносильно сравнению  $f(k) \equiv g(k) \pmod{p}$ , что и требовалось доказать.

Возможные значения для  $p$  и  $k$  сильно ограничиваются следующим наблюдением. Так как  $\alpha^{\lambda-1} + \alpha^{\lambda-2} + \dots + \alpha + 1 = 0$ , разумеется, делится на  $h(\alpha)$ , то  $k$  и  $p$  должны удовлетворять условию

$$k^{\lambda-1} + k^{\lambda-2} + \dots + k + 1 \equiv 0 \pmod{p}, \quad (1)$$

а следовательно, и такому условию:  $k^\lambda - 1 = (k - 1)(k^{\lambda-1} + \dots + k + 1) \equiv 0$ , т. е.  $k^\lambda \equiv 1 \pmod{p}$ . Напомним теперь, что, как мы видели в доказательстве теоремы Ферма в § 1.8, для любого простого  $p$  и целого  $k \not\equiv 0 \pmod{p}$  имеется такой наименьший положительный целый показатель  $d$ , что  $k^d \equiv 1 \pmod{p}$  и для положительных целых  $j$  сравнение  $k^j \equiv 1 \pmod{p}$  имеет место в том и только в том случае, когда  $d \mid j$ . В данном случае  $d$  может равняться лишь 1 или  $\lambda$ , поскольку  $k^\lambda \equiv 1 \pmod{p}$  и  $\lambda$  простое. Если  $d = 1$ , то  $k \equiv 1 \pmod{p}$  и (1) показывает, что  $\lambda \equiv 0 \pmod{p}$ ; следовательно,  $\lambda = p$ . С другой стороны, если  $\lambda = p$ , то  $k^{\lambda-1} \equiv \equiv 1 \pmod{p}$  по теореме Ферма, и в сочетании с  $k^\lambda \equiv 1 \pmod{p}$  это дает  $k \equiv 1 \pmod{p}$ . Таким образом,  $k \equiv 1 \pmod{p}$  тогда и только тогда, когда  $p = \lambda$ . Пусть теперь  $d = \lambda$ . Так как  $k^{p-1} \equiv$

<sup>1)</sup> Обозначением  $f(k)$  нужно пользоваться осторожно, поскольку круговое целое  $f(\alpha)$  не определяет целое число  $f(k)$ , т. е. из равенства круговых целых  $f(\alpha) = F(\alpha)$  не следует равенство целых чисел  $f(k)$  и  $F(k)$  (см. упр. 11). Однако, как показывает теорема, из него вытекает сравнение  $f(k) \equiv \equiv F(k) \pmod{p}$ , так что для этого  $p$  и для этого  $k$  круговое целое  $f(\alpha)$  определяет  $f(k)$  по модулю  $p$ .

$\equiv 1 \pmod{p}$  по теореме Ферма, то это дает  $\lambda \mid (p - 1)$ , т. е.  $p \equiv 1 \pmod{\lambda}$ . Подытоживая рассуждения, получаем: простое  $h(\alpha)$ , которое делит бином, либо делит  $\lambda$ , либо делит простое  $p \equiv 1 \pmod{\lambda}$ . В первом случае целое число  $k$  в приведенной выше теореме сравнимо с 1 по модулю  $\lambda$ ; во втором случае  $k \not\equiv 1 \pmod{p}$ , но  $k^\lambda \equiv 1 \pmod{p}$ .

В первом случае  $p = \lambda$ ,  $h(\alpha)$  делит  $\alpha - 1$ , поскольку  $1 - 1 \equiv 0 \pmod{\lambda}$ . Следовательно,  $Nh(\alpha)$  делит  $N(\alpha - 1)$  (норма произведения равна произведению норм). Так как число  $N(\alpha - 1) = N(1 - \alpha)$  есть значение при  $X = 1$  полинома  $(X - \alpha)(X - \alpha^2) \dots (X - \alpha^{\lambda-1}) = X^{\lambda-1} + X^{\lambda-2} + \dots + 1$ , то  $N(\alpha - 1) = \lambda$ , и, поскольку  $Nh(\alpha) \neq 1$ , мы получаем, что  $Nh(\alpha) = \lambda$  и частное от деления  $\alpha - 1$  на  $h(\alpha)$  является единицей. Значит, для  $h(\alpha)$  остается только одна возможность: быть произведением единицы на  $\alpha - 1$ . Отсюда не следует, что  $\alpha - 1$  удовлетворяет требованию, наложенному на  $h(\alpha)$ , а именно, что оно простое. Этот факт будет доказан позже в этом параграфе.

Далее, рассмотрим сопряженные  $h(\alpha^2)$ ,  $h(\alpha^3)$ ,  $\dots$ ,  $h(\alpha^{\lambda-1})$  числа  $h(\alpha)$ . Как следует прямо из определения, каждое из них простое. (Поскольку сопряжение  $\alpha \mapsto \alpha^j$  сохраняет произведения,  $h(\alpha^j)$  делит  $f(\alpha)g(\alpha)$  в том и только в том случае, когда  $h(\alpha)$  делит  $f(\alpha^i)g(\alpha^i)$ , где  $ij \equiv 1 \pmod{\lambda}$ . Так как  $h(\alpha)$  простое, отсюда вытекает, что  $h(\alpha)$  делит  $f(\alpha^i)$  или  $g(\alpha^i)$ , а следовательно,  $h(\alpha^j)$  делит  $f(\alpha)$  или  $g(\alpha)$ .) При этом каждое из сопряженных делит бином и делит  $p$ ; следовательно, для каждого из них имеется соответствующее число  $k$ .

Если  $p = \lambda$ , то значение  $k$  должно удовлетворять условию  $k \equiv 1 \pmod{\lambda}$  во всех случаях. Следовательно, два круговых целых сравнимы по модулю  $h(\alpha^j)$  тогда и только тогда, когда они сравнимы по модулю  $h(\alpha)$ , откуда следует, что  $h(\alpha^j)$  делит  $h(\alpha)$  и  $h(\alpha)$  делит  $h(\alpha^j)$ , т. е.  $h(\alpha^j)$  есть единица, умноженная на  $h(\alpha)$ . Так как  $h(\alpha)$ , если оно существует, должно быть единицей, умноженной на  $\alpha - 1$ , то отсюда должно вытекать, что  $\alpha^2 - 1$ ,  $\alpha^3 - 1$ ,  $\dots$ ,  $\alpha^{\lambda-1} - 1$  все являются единицами, умноженными на  $\alpha - 1$ . Это прямо следует, без каких бы то ни было допущений о  $h(\alpha)$ , из формул  $\alpha^j - 1 = (\alpha - 1)(\alpha^{j-1} + \alpha^{j-2} + \dots + 1)$  и  $N(\alpha^j - 1) = N(\alpha - 1)$ .

Когда  $p \neq \lambda$ ,  $p \equiv 1 \pmod{\lambda}$ , обстановка резко изменяется. Сравнение  $\alpha \equiv k \pmod{h(\alpha)}$  влечет за собой  $\alpha^j \equiv k \pmod{h(\alpha^j)}$ . Если какое-нибудь сопряженное  $h(\alpha^j)$  числа  $h(\alpha)$  делило бы некоторое другое сопряженное  $h(\alpha^i)$ , то из сравнимости по модулю  $h(\alpha^i)$  вытекала бы сравнимость по модулю  $h(\alpha^j)$  и это давало бы  $\alpha^j \equiv k \equiv \alpha^i \pmod{h(\alpha^j)}$ ; из этого вытекало бы, что  $h(\alpha^j)$  делит

$\alpha^j - \alpha^i$ , а следовательно,  $Nh(\alpha)$  делит  $N(\alpha^j - \alpha^i) = N(\alpha^{j-i} - 1)$ ; так как  $N(\alpha^{j-i} - 1) = \lambda$ , если только не имеет места  $\alpha^j = \alpha^i$ , и так как  $h(\alpha)$  не делит  $\lambda$ , то это показывает, что ни одно из сопряженных числа  $h(\alpha)$  не делит другое. Это означает, что при  $p \neq \lambda$  простые делители  $h(\alpha)$ ,  $h(\alpha^2)$ , ...,  $h(\alpha^{\lambda-1})$  числа  $p$  все различны. Так как  $h(\alpha)$  делит  $p$ , то  $p = h(\alpha)q(\alpha)$ . Так как  $h(\alpha^2)$  делит  $p$ , но не делит  $h(\alpha)$ , и так как  $h(\alpha^2)$  простое, то  $h(\alpha^2)$  делит  $q(\alpha)$ , скажем  $q(\alpha) = h(\alpha^2)q_2(\alpha)$ . Так как  $h(\alpha^3)$  делит  $p = h(\alpha)h(\alpha^2)q_2(\alpha)$ , но не делит ни  $h(\alpha)$ , ни  $h(\alpha^2)$ , то оно должно делить  $q_2(\alpha)$ , откуда  $p = h(\alpha)h(\alpha^2)h(\alpha^3)q_3(\alpha)$ . Продолжая так рассуждать дальше, найдем  $p = Nh(\alpha)q_{\lambda-1}(\alpha)$ . Таким образом, целое число  $Nh(\alpha)$  в произведении с круговым целым  $q_{\lambda-1}(\alpha)$  дает целое число  $p$ . Это показывает, во-первых, что  $q_{\lambda-1}(\alpha)$  есть целое число, и, во-вторых, поскольку  $p$  простое, что  $q_{\lambda-1}(\alpha) = 1$ ,  $p = Nh(\alpha)$ . Таким образом, мы показали не только то, что  $p$  есть норма числа  $h(\alpha)$ , но и то, что равенство  $p = Nh(\alpha)$  представляет собой полное разложение числа  $p$  на различные простые сомножители. В итоге доказана следующая

**Теорема.** Если  $h(\alpha)$  есть простое круговое целое, которое делит бином  $x + \alpha^j y$  (где  $x$  и  $y$  — взаимно простые целые числа и  $\alpha^j \neq 1$ ), то  $Nh(\alpha)$  есть простое целое число, сравнимое с 0 или 1 по модулю  $\lambda$ . Если  $Nh(\alpha) = \lambda$ , то  $h(\alpha)$  и все его сопряженные отличаются от  $\alpha - 1$  на сомножитель, являющийся единицей. Если  $Nh(\alpha) = p \equiv 1 \pmod{\lambda}$ , то  $p = Nh(\alpha)$  представляет собой разложение числа  $p$  в произведение  $\lambda - 1$  различных простых сомножителей, т. е. ни один из этих сомножителей  $h(\alpha^j)$  не делит никакой другой.

Дальнейший анализ нашей задачи, т. е. вывод необходимых условий на число  $h(\alpha)$ , чтобы оно оказалось простым делителем бинома, уже не требуется, поскольку теперь возможен синтез:

**Теорема.** Если  $h(\alpha)$  — любое круговое целое, норма которого есть простое целое число, то  $h(\alpha)$  является простым и делит бином  $x + \alpha^j y$  ( $x, y$  взаимно просты,  $\alpha^j \neq 1$ ).

**Следствия.** Круговое целое  $\alpha - 1$ , как и произведение его на любую единицу, является простым. Если норма  $Nh(\alpha)$  есть простое число, то оно сравнимо с 0 или 1 по модулю  $\lambda$ . Если  $Nh_1(\alpha) = p = Nh_2(\alpha)$  есть простое число, то  $h_2(\alpha)$  есть произведение числа, сопряженного числу  $h_1(\alpha)$ , на единицу.

**Доказательство.** Первое следствие вытекает из теоремы, поскольку  $N(\alpha - 1) = \lambda$  есть простое число. Однако чтобы доказать теорему в случае  $Nh(\alpha) = \lambda$ , проще всего прямо доказать простоту числа  $\alpha - 1$ . Из того что  $\alpha - 1$  делит  $N(\alpha - 1) = \lambda$ ,

но не делит 1, как и раньше, вытекает, что целое число делится на  $\alpha - 1$ , только если оно делится на  $\lambda$ . Кроме того,  $\alpha \equiv 1 \pmod{\alpha - 1}$ . Отсюда получаем, что если  $\alpha - 1$  делит  $f(\alpha)g(\alpha)$ , то  $f(\alpha)g(\alpha) \equiv 0 \pmod{\alpha - 1}$ ,  $f(1)g(1) \equiv 0 \pmod{\alpha - 1}$ ,  $f(1)g(1) \equiv 0 \pmod{\lambda}$  (поскольку  $f(1)g(1)$  — целое число),  $f(1)$  или  $g(1) \equiv 0 \pmod{\lambda}$  (поскольку  $\lambda$  — простое),  $f(1)$  или  $g(1) \equiv 0 \pmod{\alpha - 1}$ ,  $f(\alpha)$  или  $g(\alpha) \equiv 0 \pmod{\alpha - 1}$  и  $\alpha - 1$  делит  $f(\alpha)$  или  $g(\alpha)$ . Следовательно,  $\alpha - 1$  простое. Если  $h(\alpha)$  является произвольным круговым целым, причем  $Nh(\alpha) = \lambda$ , то, поскольку  $\alpha - 1$  делит  $Nh(\alpha)$  и является простым,  $\alpha - 1$  делит одно из сопряженных числа  $h(\alpha)$ . Так как и  $\alpha - 1$ , и сопряженные числа  $h(\alpha)$  имеют норму  $\lambda$ , то частное обязано быть единицей, а значит, некоторое из сопряженных числа  $h(\alpha)$  есть единица, умноженная на  $\alpha - 1$ . Далее, само  $h(\alpha)$  есть единица, умноженная на сопряженное числа  $\alpha - 1$ , а так как все сопряженные числа  $\alpha - 1$  суть единицы, умноженные на  $\alpha - 1$ , то отсюда следует, что само  $h(\alpha)$  есть единица, умноженная на  $\alpha - 1$ . Но  $\alpha - 1$  простое, поэтому и  $h(\alpha)$  простое, и теорема в случае  $Nh(\alpha) = \lambda$  доказана.

Второе следствие вытекает из данной и предшествующей теоремы. Однако и здесь проще провести прямое доказательство следствия как часть доказательства теоремы. Поскольку  $\alpha - 1$  есть единственный простой делитель числа  $\lambda$ , то для того, чтобы сосчитать  $Nh(\alpha) = p$  по модулю  $\lambda$ , естественно рассмотреть его по модулю  $\alpha - 1$ . Так как каждое сопряженное числа  $\alpha$  сравнимо с 1 по модулю  $\alpha - 1$ , то каждое сопряженное числа  $h(\alpha)$  сравнимо с  $h(1)$  по модулю  $\alpha - 1$  и  $p = Nh(\alpha) \equiv [h(1)]^{\lambda-1} \pmod{\alpha - 1}$ . Так как два целых числа сравнимы по модулю  $\alpha - 1$  тогда и только тогда, когда они сравнимы по модулю  $\lambda$ , получаем  $p \equiv [h(1)]^{\lambda-1} \pmod{\lambda}$ , откуда  $p \equiv 0$  или  $1 \pmod{\lambda}$  по теореме Ферма.

Основной шаг доказательства — показать, что если  $Nh(\alpha)$  — простое число, то  $h(\alpha)$  должно делить бином. Нам требуется показать, что  $h(\alpha)$ , будучи простым, должно делить бином. Если это так, то по первой теореме этого параграфа  $\alpha \equiv k \pmod{h(\alpha)}$  для некоторого целого  $k$ . Значит,  $h(\alpha)$  должно на самом деле делить бином специального вида  $\alpha - k$ . Естественно попытаться доказать это, найдя такое целое  $k$ , что  $h(\alpha)$  делит  $\alpha - k$ . Это можно сделать следующим образом.

Поскольку из  $\alpha \equiv k \pmod{h(\alpha)}$  вытекает  $1 = \alpha^\lambda \equiv k^\lambda \pmod{h(\alpha)}$ , должно иметь место сравнение  $k^\lambda - 1 \equiv 0 \pmod{p}$ , так как иначе существовали бы такие целые  $a$  и  $b$ , что  $1 = a(k^\lambda - 1) + bp$ , и это повлекло бы за собой  $1 \equiv 0 \pmod{h(\alpha)}$  вопреки предположению, что  $Nh(\alpha) = p \neq 1$ . Поэтому мы ограничимся лишь теми  $k$ , которые удовлетворяют сравнению  $k^\lambda \equiv 1 \pmod{p}$ . Пусть  $\gamma$  — примитивный корень по

модулю  $p$  (см. приложение, § A.2). Тогда каждое ненулевое по модулю  $p$  число можно единственным образом представить в виде  $\gamma^i$  ( $i = 1, 2, \dots, p-1$ ), причем  $(\gamma^i)^\lambda \equiv 1 \pmod{p}$  в том и только в том случае, когда  $p-1$  делит  $i\lambda$ . В случае  $p = \lambda$  теорема уже доказана, и так как мы знаем, что  $p \equiv 0$  или  $1 \pmod{\lambda}$ , то в оставшейся части доказательства можно считать, что  $p \equiv 1 \pmod{\lambda}$ , скажем  $p-1 = \mu\lambda$ . Тогда  $(\gamma^i)^\lambda \equiv 1 \pmod{p}$  в том и только в том случае, когда  $(p-1)/\lambda = \mu$  делит  $i$ , т. е. в том и только в том случае, когда  $i$  принимает одно из следующих значений:  $\mu, 2\mu, 3\mu, \dots, \lambda\mu = p-1$ . Пусть  $t$  есть  $\gamma^\mu$ . Тогда  $k = t, k = t^2, k = t^3, \dots, k = t^\lambda \equiv 1 \pmod{p}$  суть  $\lambda$  различных решений сравнения  $k^\lambda \equiv 1 \pmod{p}$  и каждое решение этого сравнения сравнимо по модулю  $p$  с одним из этих. (Другое доказательство того, что сравнение  $k^\lambda \equiv 1 \pmod{p}$  имеет точно  $\lambda$  решений, различных по модулю  $p$ , см. в упр. 10.) Таким образом, задача нахождения такого целого  $k$ , что  $h(\alpha)$  делит  $\alpha - k$ , сводится к задаче нахождения такого целого  $j$ , что  $h(\alpha)$  делит  $\alpha - t^j$  ( $j = 1, 2, \dots, \lambda$ ). Если  $j$  — такое целое число, то  $0 \equiv \alpha - t^j \equiv h(\alpha) \equiv h(t^j) \pmod{h(\alpha)}$ , откуда, как и раньше,  $h(t^j) \equiv 0 \pmod{p}$ . Тот факт, что имеется по крайней мере одно  $j$  в последовательности  $j = 1, 2, \dots, \lambda-1$ , для которого это необходимое условие выполняется, вытекает из следующей леммы.

**Лемма.** В предыдущих обозначениях имеет место сравнение

$$h(t) h(t^2) \dots h(t^{\lambda-1}) \equiv 0 \pmod{p}.$$

В первый момент может показаться, что лемма сразу следует из  $Nh(\alpha) = p$ , если просто положить здесь  $\alpha = t$  и перейти к сравнению по модулю  $p$ . Однако, как выше отмечалось, операция подстановки  $\alpha = t$  для круговых целых недостаточно корректно определена. Указанное рассуждение можно сделать обоснованным, если рассматривать  $h(\alpha)$  как полином от  $\alpha$  — чтобы это подчеркнуть, будем писать  $h(X)$  — и разделить полином  $h(X) \times \dots \times h(X^{\lambda-1})$  на полином  $X^{\lambda-1} + X^{\lambda-2} + \dots + 1$ , представив его в виде  $q(X)(X^{\lambda-1} + X^{\lambda-2} + \dots + 1) + r(X)$ , где  $r(X)$  — полином степени  $< \lambda-1$ . Если в этом полиномиальном тождестве положить  $X = \alpha$ , то получим  $p = q(\alpha) \cdot 0 + r(\alpha)$ , откуда, поскольку  $r(\alpha)$  имеет степень  $< \lambda-1$ , находим, что (в силу основных свойств круговых целых, перечисленных в предыдущем параграфе)  $r(X)$  есть полином  $r(X) = p$  степени 0. Положим теперь  $X = t$ ; тогда целое число, стоящее в левой части сравнения в формулировке леммы, оказывается равным  $q(t)(t^{\lambda-1} + t^{\lambda-2} + \dots + t + 1) + p$ . Для доказательства леммы достаточно показать, что  $t^{\lambda-1} + t^{\lambda-2} + \dots + 1 \equiv 0 \pmod{p}$ , а это следует из  $t^{\lambda-1} + t^{\lambda-2} + \dots + 1 = (t^\lambda - 1)/(t - 1)$ , поскольку  $t^\lambda \equiv 1 \pmod{p}$ , но  $t \not\equiv 1 \pmod{p}$ .



Итак, по крайней мере одно значение из  $j = 1, 2, \dots, \lambda - 1$  удовлетворяет необходимому условию  $h(m^j) \equiv 0 \pmod{p}$  для того, чтобы  $h(\alpha)$  делило  $\alpha - m^j$ . Теперь мы докажем, что это условие и достаточно. На основании способа деления из предыдущего параграфа определить, делит ли  $h(\alpha)$  число  $\alpha - m^j$ , — это то же самое, что определить, делит ли  $p = Nh(\alpha)$  число  $(\alpha - m^j)h(\alpha^2)h(\alpha^3)\dots h(\alpha^{\lambda-1})$ . Проведя деление с остатком полинома  $h(X)$  на  $X - m^j$ , найдем  $h(X) = q(X)(X - m^j) + r$ , где  $r$  — целое число. Полагая  $X = m^j$ , имеем  $h(m^j) = r$ . Таким образом,  $r \equiv 0 \pmod{p}$  по предположению и  $h(\alpha^v) \equiv q(\alpha^v) \times (\alpha^v - m^j) \pmod{p}$  для  $v = 1, 2, \dots, \lambda - 1$ . Значит,  $(\alpha - m^j)h(\alpha^2)h(\alpha^3)\dots h(\alpha^{\lambda-1}) \equiv (\alpha - m^j)q(\alpha^2)(\alpha^2 - m^j) \times q(\alpha^3)(\alpha^3 - m^j)\dots q(\alpha^{\lambda-1})(\alpha^{\lambda-1} - m^j) = N(\alpha - m^j)q(\alpha^2) \times q(\alpha^3)\dots q(\alpha^{\lambda-1}) \pmod{p}$ . Так как для любого целого  $k$  норма числа  $\alpha - k$  является значением при  $X = k$  полинома  $(X - \alpha)(X - \alpha^2)\dots(X - \alpha^{\lambda-1}) = X^{\lambda-1} + X^{\lambda-2} + \dots + 1 = (X^\lambda - 1)/(X - 1)$ , т. е.

$$N(\alpha - k) = \frac{k^\lambda - 1}{k - 1},$$

то  $N(\alpha - m^j) \equiv 0 \pmod{p}$  и  $h(\alpha)$  делит  $\alpha - m^j$ , что и требовалось показать.

Итак, доказано, что если целое число  $Nh(\alpha)$  простое, то  $h(\alpha)$  не только делит какой-то бином, но даже делит бином вида  $\alpha - k$ . Для завершения доказательства теоремы остается установить, что  $h(\alpha)$  простое. Для этого можно использовать те же соображения, что и раньше. Именно, если  $h(\alpha)$  делит  $f(\alpha)g(\alpha)$ , то  $f(\alpha)g(\alpha) \equiv 0 \pmod{h(\alpha)}$ ,  $f(k)g(k) \equiv 0 \pmod{h(\alpha)}$  [поскольку  $\alpha \equiv k \pmod{h(\alpha)}$ ],  $f(k)g(k) \equiv 0 \pmod{p}$  [поскольку иначе 1 можно было бы записать в виде комбинации чисел  $f(k)g(k)$  и  $p$ , что давало бы  $1 \equiv 0 \pmod{h(\alpha)}$ ],  $f(k)$  или  $g(k) \equiv 0 \pmod{p}$  (из-за простоты  $p$ ),  $f(k)$  или  $g(k) \equiv 0 \pmod{h(\alpha)}$  и, наконец,  $f(\alpha)$  или  $g(\alpha) \equiv 0 \pmod{h(\alpha)}$ , что и требовалось показать. Это завершает доказательство теоремы.

Третье следствие получится, если заметить, что  $h_2(\alpha)$  делит  $p = Nh_1(\alpha)$ , откуда из-за простоты  $h_2(\alpha)$  вытекает, что  $h_2(\alpha)$  делит одно из сопряженных числа  $h_1(\alpha)$ . Так как оба наши числа имеют норму  $p$ , то частное имеет норму 1, и  $h_2(\alpha)$  оказывается произведением единицы на сопряженное числа  $h_1(\alpha)$ , что и требовалось доказать.

Доказанная теорема применяется в следующем параграфе для нахождения большого числа простых круговых целых при малых значениях  $\lambda$ . Исторически это и есть тот путь, которым следовал Куммер в 1844 г. При этом он допустил серьезную ошибку, считая доказанным, что каждое простое  $p \equiv 1 \pmod{\lambda}$  является нормой



некоторого кругового целого. Это утверждение неверно: например, как покажут вычисления в следующем параграфе, при  $\lambda = 23$  число  $47 = 2 \cdot 23 + 1$  не является нормой никакого кругового целого. Удивительно, что Куммер сам этого не обнаружил в процессе своих вычислений. Первым, кто заметил, что имеется совершенно очевидная причина, по которой уравнение  $Nh(\alpha) = p$  не всегда разрешимо, даже если  $p \equiv 1 \pmod{\lambda}$ , был, видимо, Якоби (подробнее см. [E4]). К счастью для Куммера, Якоби вовремя предупредил его об этой ошибке, и он смог приостановить публикацию своей работы с неверной теоремой. Думается, Куммеру повезло также и в том, что он не нашел своей ошибки *слишком быстро*. Это позволило ему достаточно далеко углубиться в свою теорию и, видимо, внести в нее столь ощутимый вклад, что у него хватило сил преодолеть встретившиеся трудности и продолжать создание теории, которая обеспечила ему важное место в истории математики.

## Упражнения

1. Докажите, что если  $h(\alpha)$  простое, то оно неразложимо.
2. Докажите, что обычное положительное целое число  $n$ , которое неразложимо (из  $n = mk$  вытекает, что  $m$  или  $k$  равно 1), является простым (из  $n \mid mk$  вытекает, что  $n \mid m$  или  $n \mid k$ ).
3. Докажите, что если  $h(\alpha)$  неразложимо, но не просто, то имеется круговое целое, которое может быть записано в виде произведения неразложимых двумя различными способами. Такими образом, если из неразложимости не вытекает простота, то единственность разложения не имеет места. [Предположите, что каждое круговое целое может быть записано в виде произведения неразложимых.]
4. Найдите нормы следующих биномов. (a) При  $\lambda = 5$ :  $x + \alpha y = 1 + \alpha, 2 + \alpha, 2 - \alpha, 3 + \alpha, 3 - \alpha, 3 + 2\alpha, 3 - 2\alpha, 4 + \alpha, 5 + 2\alpha, 5 - 4\alpha, 7 + \alpha$ . (b) При  $\lambda = 7$ :  $x + \alpha y = 2 \pm \alpha, 3 \pm \alpha, 3 \pm 2\alpha, 4 \pm \alpha, 4 \pm 3\alpha, 5 + \alpha, 5 + 2\alpha, 5 + 3\alpha, 5 + 4\alpha$ . [ $N(x + \alpha y) = (x^\lambda + y^\lambda)/(x + y)$ .]
5. В тексте было доказано, что если  $p$  делит  $N(x + \alpha y)$ , где  $x$  и  $y$  взаимно просты, и имеет простой делитель  $h(\alpha)$ , то  $p \equiv 0$  или  $1 \pmod{\lambda}$ . Докажите, что предположение о простом делителе  $h(\alpha)$  не нужно. [Используйте формулу для  $N(x + \alpha y)$ .]
6. Используя факт, доказанный в упр. 5, разложите нормы, найденные в упр. 4.
7. При  $\lambda = 5$  найдите норму  $N(9 - \alpha)$  (a) непосредственно; (b) заметив, что она равна  $N(3 - \alpha)N(3 + \alpha)$ .
8. Докажите, что если  $p \equiv 1 \pmod{\lambda}$  и  $h_1(\alpha), h_2(\alpha)$  — простые делители числа  $p$ , то  $h_2(\alpha)$  есть произведение единицы на сопряженное числа  $h_1(\alpha)$ . Иными словами, разложение числа  $p$  на простые, если оно существует, единственно.
9. Суть последней теоремы из текста в том, что если  $h(\alpha)$  имеет нормой простое число, то  $\alpha \equiv k \pmod{h(\alpha)}$  при некотором целом  $k$ . Куммер доказал эту важную теорему в своей статье 1844 г. Однако его доказательство было совсем другим. Восполните детали следующих рассуждений. Пусть  $h(\alpha^2)h(\alpha^3)\dots h(\alpha^{\lambda-1}) = H(\alpha) = A_0 + A_1\alpha + A_2\alpha^2 + \dots + A_{\lambda-1}\alpha^{\lambda-1}$ . Тогда  $\alpha^{-n}H(\alpha) + \alpha^{-2n}H(\alpha^2) + \dots + \alpha^{-(\lambda-1)n}H(\alpha^{\lambda-1}) = \lambda A_n - (A_0 + A_1 + \dots$

$+ A_{\lambda-1})$  и  $\alpha^{-n} (1-\alpha) H(\alpha) + \alpha^{-2n} (1-\alpha^2) H(\alpha^2) + \dots + \alpha^{-(\lambda-1)n} (1 - \alpha^{\lambda-1}) H(\alpha^{\lambda-1}) = \lambda (A_n - A_{n-1})$ . Так как  $H(\alpha^j) H(\alpha^k) \not\equiv 0 \pmod{p}$  при  $j \neq k$ , то это дает  $\lambda^2 (A_{n+1} - A_n)^2 - \lambda^2 (A_{n+2} - A_{n+1}) (A_n - A_{n-1}) \equiv 0 \pmod{p}$ . Значит, решение  $\xi$  сравнения  $(A_{n+2} - A_{n+1}) \xi \equiv A_{n+1} - A_n$  одно и то же для всех  $n$ . Следовательно,  $A_{n+1}\xi - A_n$  одно и то же по модулю  $p$  для всех  $n$ ,  $(\xi - \alpha) H(\alpha)$  есть нуль по модулю  $p$  и, таким образом,  $h(\alpha)$  делит  $\alpha - \xi$ .

10. Применяя теоремы этого параграфа, покажите, что если  $p \equiv 1 \pmod{\lambda}$  является простым числом, которое делится на круговое целое  $h(\alpha)$ , то имеется точно  $\lambda - 1$  различных решений сравнения  $k^\lambda \equiv 1$ ,  $k \not\equiv 1 \pmod{p}$  и все они являются степенями любого одного из них. [Рассмотрите целые, сравнимые с  $\alpha^j$  по модулю  $h(\alpha)$ .] Докажите, что это верно без предположения о простом делителе  $h(\alpha)$ . [Примените теорему Ферма.]

11. При  $\lambda = 5$  имеем  $0 = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$ , но, разумеется,  $0 \neq 1 + 7 + 7^2 + 7^3 + 7^4$ . Значит, из  $f(\alpha) = g(\alpha)$  не следует, что  $f(7) = g(7)$ . По каким простым модулям  $p$  имеет место сравнение  $f(7) \equiv g(7) \pmod{p}$ ?

12. Докажите, что  $f(\alpha) = g(\alpha)$  тогда и только тогда, когда  $f(X) - g(X) = q(X) (X^{\lambda-1} + X^{\lambda-2} + \dots + 1)$ . Установите, что если  $k^{\lambda-1} + k^{\lambda-2} + \dots + 1 \equiv 0 \pmod{p}$ , то из  $f(\alpha) = g(\alpha)$  следует  $f(k) \equiv g(k) \pmod{p}$ .

#### 4.4. Вычисления для $p \equiv 1 \pmod{\lambda}$

Оказывается, среди математиков существует глубоко укоренившаяся тенденция неосознанно предполагать единственность разложения на простые. Эта тенденция, несомненно, навеяна опытом вычислений с обычными целыми числами и той важной ролью, которую играет единственность разложения в доказательстве таких фактов, как утверждение о том, что произведение двух взаимно простых чисел есть квадрат только тогда, когда каждый сомножитель является квадратом. Свидетельством силы этой тенденции служит использование Эйлером в его «Алгебре» единственности разложения для квадратичных целых, несмотря на контрпример  $3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$ , известный как ему, так и за сто лет до него Пьеру Ферма в виде утверждения, что простой делитель целого числа, представимого в виде  $a^2 + 5b^2$ , не обязательно сам имеет такой вид (см. § 1.7 и 2.5). В случае круговых целых эта тенденция *подкрепляется* на опыте вычислений, поскольку при  $\lambda < 23$  единственность разложения для круговых целых действительно *имеет место*. Поэтому не приходится удивляться, что Ламе был твердо уверен в единственности разложения для круговых целых: «Не может быть непреодолимого препятствия между таким полным подтверждением и строгим доказательством». Конечно, Куммер также испытывал большую надежду — если не уверенность, — что единственность разложения для круговых целых имеет место, и именно по этой причине он счел весьма прискорбным свое открытие ее нарушения для  $\lambda = 23$ . Если бы вера Куммера в единственность разложения не подтверждалась так долго опытом вычислений, то вряд ли он стал бы искать пути ее спасения и ему едва ли удалось создать теорию в том виде, в каком мы знаем ее сейчас. На самом деле имеются некоторые, правда косвенные, свидетельства (но относящиеся ко временам Гаусса), что сам Гаусс пытался создать нечто подобное теории Куммера для случая квадратичных целых (чисел вида  $a + b\sqrt{D}$ , где  $D$  фиксировано), но что он оказался не в состоянии разработать детали и опубликовал свои результаты (в *Disquisitiones Arithmeticae*) только в совсем другом и более запутанном виде «композиции форм» (см. § 8.6).

Опубликованные Ламе вычисления совсем не велики и при трезвом взгляде никак не оправдывают его убеждения в единственности разложения.

Однако они действительно служат хорошим отправным пунктом исследования некоторых вычислительных примеров. При помощи формулы

$$N(x + \alpha y) = \frac{x^\lambda + y^\lambda}{x + y}$$

он находит в [L6] нормы следующих <sup>1)</sup> биномов в случае  $\lambda = 5$ :

- |                                  |                                     |
|----------------------------------|-------------------------------------|
| (1) $N(\alpha + 2) = 11$         | (6) $N(2\alpha + 5) = 11 \cdot 41$  |
| (2) $N(\alpha - 2) = 31$         | (7) $N(\alpha - 4) = 11 \cdot 31$   |
| (3) $N(\alpha + 3) = 61$         | (8) $N(\alpha - 9) = 11^2 \cdot 61$ |
| (4) $N(\alpha + 4) = 5 \cdot 41$ | (9) $N(4\alpha - 5) = 11 \cdot 191$ |
| (5) $N(\alpha - 3) = 11^2$       | (10) $N(\alpha + 7) = 11 \cdot 191$ |

В свете теорем предыдущего параграфа первое из этих равенств показывает, что  $\alpha + 2$  простое, что круговое целое  $g(\alpha)$  делится на  $\alpha + 2$  в том и только в том случае, когда  $g(-2) \equiv 0 \pmod{11}$ , и что равенство  $N(\alpha + 2) = 11$  является представлением числа 11 в виде произведения 4 различных простых сомножителей, норма каждого из которых равна 11. Сходным образом, равенства (2) и (3) дают разложения чисел 31 и 61 в произведения 4 различных простых сомножителей.

Равенство (4) указывает, что  $\alpha + 4$  есть произведение сомножителя с нормой 5 и сомножителя с нормой 41. Единственными сомножителями нормы 5 ( $= \lambda$ ) являются единицы, умноженные на  $\alpha - 1$ . Поэтому разделим  $\alpha + 4 = \alpha - 1 + 5$  на  $\alpha - 1$  и найдем частное  $1 + (\alpha^2 - 1)(\alpha^3 - 1) \times (\alpha^4 - 1)$  [поскольку  $5 = N(\alpha - 1) = 1 + (1 - \alpha^2 - \alpha^3 + 1)(\alpha^4 - 1) = 1 + 2\alpha^4 - \alpha - \alpha^2 - 2 + \alpha^2 + \alpha^3 = -1 - \alpha + \alpha^3 + 2\alpha^4 = \alpha^2 + 2\alpha^3 + 3\alpha^4$  [так как  $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$ ]]. Таким образом,  $\alpha + 4 = (\alpha - 1)\alpha^2(3\alpha^2 + 2\alpha + 1)$ . Конечно,  $\alpha^2$  есть единица. Отсюда вытекает, что  $3\alpha^2 + 2\alpha + 1$  имеет норму 41 и, следовательно, является простым. Так как  $3\alpha^2 + 2\alpha + 1$  делит  $\alpha + 4$ , то  $\alpha \equiv -4 \pmod{(3\alpha^2 + 2\alpha + 1)}$ , и сравнение  $f(\alpha) \equiv g(\alpha) \pmod{(3\alpha^2 + 2\alpha + 1)}$  равносильно сравнению  $f(-4) \equiv g(-4) \pmod{41}$ .

Равенство (5) показывает, что каждый простой делитель числа 11 делит некоторое из сопряженных числа  $\alpha - 3$ . Простое  $\alpha + 2$  само делит  $\alpha^3 - 3$ , поскольку  $(-2)^3 - 3 \equiv 0 \pmod{11}$ . Следовательно,  $\alpha^2 + 2$  делит  $\alpha - 3 = (\alpha^2)^3 - 3$  и частное имеет норму 11. Следовательно, частное есть единица, умноженная на один из четырех простых делителей вида  $\alpha^j + 2$  числа 11. Так как  $\alpha + 2$  не делит  $\alpha - 3$ ,  $\alpha^2 - 3$ ,  $\alpha^4 - 3$ , то единственное из его сопряженных, делящее  $\alpha - 3$ , есть  $\alpha^2 + 2$ , и это дает  $\alpha - 3 = \text{единица} \cdot (\alpha^2 + 2)^2$ .

Равенство (6) показывает, что  $2\alpha + 5$  делится на простой делитель числа 11 и на простой делитель числа 41. Сопряженное числа  $2\alpha + 5$ , которое делится на  $\alpha + 2$ , есть  $2\alpha^3 + 5$ , так как  $2 \cdot (-2)^3 + 5 \equiv 0 \pmod{11}$ . Аналогично, сопряженное числа  $2\alpha + 5$ , делящееся на  $3\alpha^2 + 2\alpha + 1$ , находится перебором:  $-4, 16, -64 \equiv 18, (-4) \cdot 18 = -72 \equiv 10 \pmod{41}$ ; получаем  $0 \equiv 2 \cdot 18 + 5 \equiv 2 \cdot (-4)^3 + 5 \pmod{41}$ ; таким образом,  $2\alpha^3 + 5$  и есть то, которое делится. Следовательно,  $2\alpha^3 + 5 = \text{единица} \cdot (\alpha + 2)(3\alpha^2 + 2\alpha + 1)$ , что дает представление  $2\alpha + 5 = \text{единица} \cdot (\alpha^2 + 2)(3\alpha^4 + 2\alpha^2 + 1)$  числа  $2\alpha + 5$  в виде произведения простых.

Равенства (7) и (8) непосредственно следуют из разложений  $\alpha^2 - 4 = (\alpha - 2)(\alpha + 2)$ ,  $\alpha^2 - 9 = (\alpha - 3)(\alpha + 3)$ , которые дают  $\alpha - 4 = (\alpha^3 - 2)(\alpha^3 + 2)$ ,  $\alpha - 9 = (\alpha^3 - 3)(\alpha^3 + 3)$ . Первое из этих равенств есть разложение на простые сомножители. Второе можно продолжить, исполь-

<sup>1)</sup> Ламе пользуется совсем другими обозначениями, но их легко переосмыслить.

зую разложение  $\alpha - 3 = \text{единица} \cdot (\alpha^2 + 2)^2$  и получая  $\alpha - 9 = \text{единица} \times (\alpha + 2)^2 (\alpha^3 + 3)$ .

Равенство (9) показывает, что  $\alpha + 2$  делит некоторое из сопряженных числа  $4\alpha - 5$ . То, которое оно делит, есть  $4\alpha^2 - 5$ . Частное равно

$$\begin{aligned} 4\alpha - 8 + 11(\alpha + 2)^{-1} &= 4\alpha - 8 + (\alpha^2 + 2)(\alpha^3 + 2)(\alpha^4 + 2) = \\ &= 4\alpha - 8 + (1 + 2\alpha^2 + 2\alpha^3 + 4)(\alpha^4 + 2) = \\ &= 4\alpha - 8 + 5\alpha^4 + 2\alpha + 2\alpha^2 + 10 + 4\alpha^2 + 4\alpha^3 = \\ &= 2 + 6\alpha + 6\alpha^2 + 4\alpha^3 + 5\alpha^4 = -4 - 2\alpha^3 - \alpha^4. \end{aligned}$$

Следовательно,  $\alpha^4 + 2\alpha^3 + 4$  имеет норму 191 и поэтому простое. Таким образом,  $4\alpha - 5 = -(\alpha^3 + 2)(2\alpha^4 + \alpha^2 + 4)$  есть разложение числа  $4\alpha - 5$  на простые. Целое  $k$ , для которого  $\alpha \equiv k \pmod{(2\alpha^4 + \alpha^2 + 4)}$ , удовлетворяет условию  $4k - 5 \equiv 0 \pmod{191}$ , откуда  $k \equiv 192k = 48 \cdot 4k \equiv 48 \cdot 5 = 48 \cdot 4 + 48 \equiv 49 \pmod{191}$ . Таким образом,  $g(\alpha)$  делится на  $2\alpha^4 + \alpha^2 + 4$  тогда и только тогда, когда  $g(49) \equiv 0 \pmod{191}$ .

Наконец, равенство (10) показывает, что  $\alpha + 7$  делится на делитель числа 11 и на делитель числа 191. Путем кратких вычислений получаем  $49^2 \equiv -82 \pmod{191}$ ,  $49^3 \equiv -82 \cdot 49 \equiv -7 \pmod{191}$ . Значит,  $\alpha^3 + 7$  делится на  $2\alpha^4 + \alpha^2 + 4$ . С другой стороны,  $\alpha^2 + 7$  делится на  $\alpha + 2$ . Следовательно,  $\alpha + 7 = \text{единица} \cdot (\alpha^3 + 2) \cdot (2\alpha^3 + \alpha^4 + 4)$ , что представляет собой разложение числа  $\alpha + 7$  на простые сомножители.

Простые делители, найденные до сих пор, приведены в табл. 4.4.1. Разобранные примеры показывают, что для определения делимости полезно

Таблица 4.4.1.  $\lambda = 5$

простое	норма	$\alpha \equiv$	$\alpha^2 \equiv$	$\alpha^3 \equiv$	$\alpha^4 \equiv$
$\alpha + 2$	11	-2	4	3	5
$\alpha - 2$	31	2	4	8	-15
$3\alpha^2 + 2\alpha + 1$	41	-4	16	18	10
$\alpha + 3$	61	-3	9	-27	20
$2\alpha^4 + \alpha^2 + 4$	191	49	-82	-7	39

знать не только величину целого  $k$  по модулю  $p$ , но и его степени. Поэтому эти степени, которые представляют собой целые числа, сравнимые с  $\alpha^2$ ,  $\alpha^3$  и  $\alpha^4$  по рассматриваемому простому модулю, включены в таблицу. Заметим, что каждая строка таблицы дает на самом деле *четыре* простых круговых целых; мы берем сопряженные данного простого и соответственно переставляем степени числа  $\alpha$ . Например,  $\alpha^2 + 2$  простое и для этого простого делителя  $\alpha^2 \equiv -2$ ,  $\alpha^4 \equiv 4$ ,  $\alpha^6 = \alpha \equiv 3$ ,  $\alpha^8 = \alpha^3 \equiv 5$ .

Ламе выполнил подобные разложения для каждого из своих равенств (1) — (10), хотя сделал много ошибок. Затем он сказал, что если и дальше продолжать рассматривать биномы  $x\alpha + y$ , то можно найти разложения еще многих простых  $p \equiv 1 \pmod{5}$ . Хотя это и верно<sup>1)</sup>, но в таком контексте вводит в заблуждение, поскольку тот же самый процесс *не* позволяет разлагать простые  $p \equiv 1 \pmod{\lambda}$  при  $\lambda > 5$ . Чтобы понять, почему это происходит, рассмотрим случай  $\lambda = 7$ .

<sup>1)</sup> Кажется, Ламе пытался создать впечатление, что он провел более длинные выкладки, чем это было на самом деле. Он говорит, что, «за несколькими исключениями», каждое простое  $\equiv 1 \pmod{5}$  вплоть до 1021 встречается в качестве делителя числа  $N(x\alpha + y)$  для некоторой пары  $x, y$  при  $|x| \leq 12$ ,  $|y| \leq 12$ . Первые 23 таких простых числа, вплоть до 521, действительно все встречаются. Однако из остальных восемнадцати, до 1021, встречаются всего лишь 6.

Здесь нормы нескольких первых биномов, найденные по формуле

$$N(x\alpha + y) = \frac{x^7 + y^7}{x + y},$$

равны

$$N(\alpha + 2) = 43$$

$$N(\alpha - 2) = 127$$

$$N(\alpha + 3) = 547$$

$$N(\alpha - 3) = 1093$$

$$N(2\alpha + 3) = 463$$

$$N(2\alpha - 3) = 2059 = 29 \cdot 71$$

$$N(\alpha + 4) = 3277 = 29 \cdot 113$$

$$N(\alpha - 4) = 5461 = 43 \cdot 127$$

$$N(3\alpha + 4) = 2653 = 7 \cdot 379$$

$$N(3\alpha - 4) = 14197.$$

(Поскольку единственными возможными простыми сомножителями являются 7, 29, 43, 71, 113, . . . , приведенные разложения легко находятся, и легко доказать, что те числа, которые не разложены, простые.) Если попытаться имитировать метод Ламе, то сразу становится понятно, что его успех в случае  $\lambda = 5$  обеспечивался тем, что в этом случае список начинался с разложений простых 11, 31, 61 и с разложения 5·41, что равносильно разложению простого 41. В случае же  $\lambda = 7$  мы находим разложения для простых 43 и 127, а для 29, 71 и 113 не находим. Нормы быстро растут, и ясно, что нет никакой надежды найти бином с нормой, скажем, 29. Значит, для разложения числа 29 нужно прибегнуть к какой-то другой технике.

Техника, которую развил Куммер в своей статье 1844 г., заключалась в том, чтобы *сначала отыскивать значения  $k$* , после чего нетрудно находить круговые целые, *делящиеся* на искомые простые, а если повезет, то удастся найти и сами искомые простые. В случае  $\lambda = 7$ ,  $p = 29$ , любая четвертая степень  $k = a^4$  удовлетворяет сравнению  $k^7 = a^{29-1} \equiv 1 \pmod{29}$ ,  $k \not\equiv 1 \pmod{29}$  при условии, что  $a \not\equiv 0 \pmod{29}$  и  $a^4 \not\equiv 1 \pmod{29}$ . При  $a = 2$  находим  $k = 16 \equiv -13 \pmod{29}$  и имеет место сравнение  $(-13)^7 \equiv 1 \pmod{29}$ . Другие значения для  $k \not\equiv 1$ ,  $k^7 \equiv 1 \pmod{29}$  получаются из  $(-13)^2 \equiv -5$ ,  $(-13)^3 \equiv 7$ ,  $(-13)^4 \equiv -4$ ,  $(-13)^5 \equiv -6$ ,  $(-13)^6 \equiv -9$ . Если 29 *имеет* разложение на простые, то один из сомножителей  $h(\alpha)$  должен обладать свойством:  $h(\alpha)$  делит  $g(\alpha)$  тогда и только тогда, когда  $g(-13) \equiv 0 \pmod{29}$ . Но из приведенной выше таблицы значений степеней числа  $-13$  по модулю 29 видно, что  $g(\alpha) = \alpha^2 - \alpha^4 + 1$  удовлетворяет сравнению  $g(-13) \equiv 0 \pmod{29}$ . Следовательно, такое  $g(\alpha)$  делится на предполагаемый делитель числа 29. Так как норма этого гипотетического делителя есть 29, то норма частного равна  $Ng(\alpha)/29$ . Простое вычисление показывает<sup>1)</sup>, что  $Ng(\alpha) = 29$ . Значит,  $g(\alpha)$  само простое, поэтому равенство  $Ng(\alpha) = 29$  и дает разложение на простые сомножители числа 29.

Разложения чисел 71 и 113 теперь можно найти посредством деления  $2\alpha - 3$  и  $\alpha + 4$  соответственно на подходящий делитель числа 29. Так как  $2k - 3 \equiv 0 \pmod{29}$  для  $k = -13$ , то  $2\alpha - 3$  делится на  $-\alpha^4 + \alpha^2 + 1$ . Частное равно  $(2\alpha - 3)g(\alpha^2) \cdot g(\alpha^3)g(\alpha^4) \cdot g(\alpha^5)g(\alpha^6)/29 = (2\alpha - 3)g(\alpha^2) \times \times g(\alpha^4)f(\alpha^3)/29$ , где обозначение  $f(\alpha)$  введено в предыдущем примечании,

<sup>1)</sup> Для дальнейшего полезно сделать следующее замечание о вычислении нормы  $Ng(\alpha) = g(\alpha)g(\alpha^2)g(\alpha^3)g(\alpha^4)g(\alpha^5)g(\alpha^6)$ . Так как 3 есть примитивный корень по модулю 7 (см. приложение, § А.2), то повторения одного сопряжения  $\alpha \mapsto \alpha^3$  исчерпывают все сопряжения. Поэтому сомножители в  $Ng(\alpha)$  можно записать в таком порядке  $g(\alpha)g(\alpha^3)g(\alpha^2)g(\alpha^6)g(\alpha^4) \times \times g(\alpha^5)$ , где каждый сомножитель сопряжен предшествующему под действием  $\alpha \mapsto \alpha^3$ . Далее, если мы определим  $f(\alpha)$  как произведение сомножителей, стоящих на нечетных местах, т. е.  $f(\alpha) = g(\alpha)g(\alpha^2)g(\alpha^4)$ , то получим  $Ng(\alpha) = f(\alpha)f(\alpha^3)$ . Этим путем вычисление нормы  $Ng(\alpha)$  сводится к трем



$= (2\alpha - 3) (-2\alpha^6 - 3\alpha^2 - \alpha) (-1 - 4\theta_1)/29 = (2\alpha - 3) (6\alpha^6 + 20\alpha^5 + 12\alpha^4 + 11\alpha^2 + 13\alpha + 16)/29 = (22\alpha^6 - 36\alpha^5 - 36\alpha^4 + 22\alpha^3 - 7\alpha^2 - 7\alpha - 36)/29 = 2\alpha^6 + 2\alpha^3 + \alpha^2 + \alpha$ . Следовательно,  $2\alpha^5 + 2\alpha^2 + \alpha + 1$  — простой делитель числа 71. Соответствующее  $k$  удовлетворяет сравнению  $2k - 3 \equiv 0 \pmod{71}$ , откуда  $k \equiv 72k \equiv 36 \cdot 2k \equiv 36 \cdot 3 = 36 \cdot 2 + 36 \equiv \equiv 37 \pmod{71}$ ; далее легко находятся  $k^2 \equiv 20$ ,  $k^3 \equiv 30$ ,  $k^4 \equiv -26$ ,  $k^5 \equiv 32$ ,  $k^6 \equiv -23 \pmod{71}$ .

Аналогично, чтобы разделить  $\alpha + 4$  на делитель числа 29, испытываем  $k + 4 \equiv 0 \pmod{29}$  при  $k = -13, -5, 7, -4, -6, -9$ . Решением является  $k = -4$ , и отсюда следует, что  $\alpha^4 + 4$  делится на  $-\alpha^4 + \alpha^2 + 1$ . Основной объем требуемой работы по такому делению был нами уже проделан раньше. Частное оказывается равным  $(\alpha^4 + 4) (6\alpha^6 + 20\alpha^5 + 12\alpha^4 + 11\alpha^2 + 13\alpha + 16)/29 = (35\alpha^6 + 93\alpha^5 + 64\alpha^4 + 6\alpha^3 + 64\alpha^2 + 64\alpha + 64)/29 = -\alpha^6 + \alpha^5 - 2\alpha^3 = -\alpha^3 (\alpha^3 - \alpha^2 + 2)$ . Таким образом,  $\alpha^3 - \alpha^2 + 2$  есть простой делитель числа 113. Соответствующее  $k$  легко находится, если использовать то, что  $\alpha^3 - \alpha^2 + 2$  делит  $\alpha^4 + 4$ ; это дает  $k^4 \equiv -4 \pmod{113}$ . Отсюда  $k \equiv \equiv k^8 \equiv 16$ ,  $k^2 \equiv 16^2 \equiv 30$  и т. д.

Следующим за 127 простым числом  $\equiv 1 \pmod{7}$  является 197. Если мы продолжим нашу таблицу норм  $N(x\alpha + y)$  немного дальше, то найдем  $N(\alpha + 6) = 39\,991 = 7 \cdot 29 \cdot 197$ . Деление числа  $\alpha + 6$  на  $\alpha - 1$  дает  $1 + 7(\alpha - 1)^{-1} = 1 + (\alpha^2 - 1)(\alpha^3 - 1)(\alpha^4 - 1)(\alpha^5 - 1)(\alpha^6 - 1)$ . Произведение  $(\alpha^2 - 1)(\alpha^3 - 1) \dots (\alpha^6 - 1)$  может быть найдено прямым умножением и равно  $6\alpha^6 + 5\alpha^5 + 4\alpha^4 + 3\alpha^3 + 2\alpha^2 + \alpha$ , что является частным случаем формулы, верной для произвольного  $\lambda$ , а именно  $(\alpha^2 - 1)(\alpha^3 - 1) \dots (\alpha^{\lambda-1} - 1) = (\lambda - 1)\alpha^{\lambda-1} + \dots + 2\alpha^2 + \alpha$  (см. упр. 11). Таким образом,  $(\alpha + 6)(\alpha - 1)^{-1} = 6\alpha^6 + 5\alpha^5 + 4\alpha^4 + 3\alpha^3 + 2\alpha^2 + \alpha + 1 = \alpha^2(5\alpha^4 + 4\alpha^3 + 3\alpha^2 + 2\alpha + 1)$ . Для того чтобы разделить это число на простой делитель числа 29, испытаем, как и раньше,  $\alpha \equiv -13, -5, 7, -4, -6, -9$  и редуцируем по модулю 29. Нуль получается при  $k = -6 \equiv \equiv (-13)^5 \pmod{29}$ . Значит,  $5\alpha^6 + 4\alpha + 3\alpha^3 + 2\alpha^5 + 1$  делится на  $-\alpha^4 + \alpha^2 + 1$ . Частное равно  $(5\alpha^6 + 4\alpha + 3\alpha^3 + 2\alpha^5 + 1)(6\alpha^6 + 20\alpha^5 + 12\alpha^4 + 11\alpha^2 + 13\alpha + 16)/29 = (192\alpha^6 + 163\alpha^5 + 163\alpha^4 + 192\alpha^3 + 105\alpha^2 + 192\alpha + 163)/29 = \alpha(\alpha^5 + \alpha^2 - 2\alpha + 1)$ . Таким образом,  $5\alpha^4 + 4\alpha^3 + 3\alpha^2 + 2\alpha + 1 = (-\alpha^5 + \alpha^6 + 1) \cdot \alpha^3 \cdot (\alpha + \alpha^6 - 2\alpha^3 + 1)$ . Итак,  $\alpha + 6 = (\alpha - 1) \cdot (\alpha^6 - \alpha^5 + 1)(\alpha^6 - 2\alpha^3 + \alpha + 1) \cdot \alpha^5$  и  $\alpha^6 - 2\alpha^3 + \alpha + 1$  есть простое с нормой 197, по модулю которого  $\alpha \equiv -6$ .

умножениям. Вычисление  $f(\alpha)$  может быть записано так:

$\alpha^6$	$\alpha^5$	$\alpha^4$	$\alpha^3$	$\alpha^2$	$\alpha$	1	$\alpha^6$	$\alpha^5$	$\alpha^4$	$\alpha^3$	$\alpha^2$	$\alpha$	1
0	0	-1	0	1	0	1	0	0	-1	-2	0	-3	0
0	0	1	0	0	-1	1					-1	1	1
<hr/>							<hr/>						
		-1		1		1			-1	-2		-3	
	1		-1		-1			-1	-2		-3		
1		1			-1		1	2		3			
<hr/>							<hr/>						
1	1	0	-1	1	-2	1	1	1	-3	1	-3	-3	0
= 0	0	-1	-2	0	-3	0							

Таким образом,  $f(\alpha) = -3\theta_0 + \theta_1 = -1 - 4\theta_0$ , где  $\theta_0 = \alpha + \alpha^2 + \alpha^4$  и  $\theta_1 = \alpha^3 + \alpha^5 + \alpha^6$ . (Поскольку  $f(\alpha) = g(\alpha)g(\alpha^2)g(\alpha^4)$  не меняется при замене  $\alpha$  на  $\alpha^2$ , ясно, что для любого  $g(\alpha)$  число  $f(\alpha)$  представимо в виде  $a\theta_0 + b\theta_1 + c$ .) Далее,  $f(\alpha^3) = -1 - 4\theta_1$  и  $Ng(\alpha) = (1 + 4\theta_0)(1 + 4\theta_1) = 1 - 4 + 16\theta_0\theta_1$ . Простое перемножение дает  $\theta_0\theta_1 = \theta_0 + \theta_1 + 3 = 2$  и  $Ng(\alpha) = -3 + 32 = 29$ .



Этот метод разложения биномов, по-видимому, не дает делителя следующего простого числа  $211 \equiv 1 \pmod{7}$ . Первый бином, норма которого делится на 211, есть  $3\alpha - 10$ , причем  $N(3\alpha - 10) = 7 \cdot 211 \cdot 967$ , и прежде чем это можно будет использовать для разложения числа 211, нужно разложить 967. Поэтому мы применим сначала метод Куммера нахождения возможных значений для  $k$  и на основе этого попытаемся найти круговые целые, *делящиеся* на гипотетический делитель числа 211, в надежде, что среди них попадется число с нормой 211. Первый шаг состоит в решении сравнения  $k \not\equiv 1, k^7 \equiv 1 \pmod{211}$ . Для этого мы можем положить  $k \equiv a^{30}$  при условии, что  $a \not\equiv 0, a^{30} \not\equiv 1 \pmod{211}$ . При  $a = 2$  находим  $a^{30} \equiv -40 \pmod{211}$ . Значит, если 211 имеет простые делители, то среди них есть такой, по модулю которого  $\alpha \equiv -40, \alpha^2 \equiv 1600 \equiv -88, \alpha^3 \equiv -67, \alpha^4 \equiv -63, \alpha^5 \equiv -12, \alpha^6 \equiv 58$ . Этот делитель должен, следовательно, делить  $\alpha^4 - \alpha^3 - 4$ . Вычисления, подобные проведенным ранее, дают  $N(\alpha^4 - \alpha^3 - 4) = 29 \cdot 211$ . Следовательно,  $\alpha^4 - \alpha^3 - 4$  можно разделить на простой делитель числа 29 и найти элемент с нормой 211, а тем самым разложение числа 211 на простые. По-другому, можно опять пытаться найти  $g(\alpha)$ , удовлетворяющее условию  $g(-40) \equiv 0 \pmod{211}$ , которое имеет норму 211. Список сумм и разностей степеней числа  $\alpha$  по модулю гипотетического простого (которое на основании предыдущих вычислений действительно существует), т. е. выражений типа  $\pm\alpha \pm \alpha^2 \equiv \pm 48, \pm 83 (\equiv \pm 128); \pm\alpha \pm \alpha^3 \equiv \pm 27, \pm 104; \pm\alpha \pm \alpha^4 \equiv \pm 23, \pm 103; \dots; \pm\alpha^5 \pm \alpha^6 \equiv \pm 46, \pm 70$ , дает 60 целых чисел по модулю 211, которые сравнимы с суммами и разностями степеней числа  $\alpha$ . Наименьшее из них есть 4, использованное раньше. Однако если взять еще другую степень числа  $\alpha$  и поискать среди этих 60 чисел наиболее близкое к какой-нибудь степени числа  $\alpha$ , то найдутся случаи, когда такая разность равна всего лишь 2. Например,  $\pm\alpha^3 \pm \alpha^6 \equiv \pm 9, \pm 86$  и  $\alpha^2 \equiv -88$  приводит к  $\alpha^6 - \alpha^3 - \alpha^2 \equiv 213 \equiv 2$ . Вычисления дают  $N(\alpha^6 - \alpha^3 - \alpha^2 - 2) = 211$ , и это завершает разложение числа 211.

Таблица 4.4.2.  $\lambda = 7$

простое	норма	$\alpha \equiv$	$\alpha^2 \equiv$	$\alpha^3 \equiv$	$\alpha^4 \equiv$	$\alpha^5 \equiv$	$\alpha^6 \equiv$
$-\alpha^4 + \alpha^2 + 1$	29	- 13	- 5	7	- 4	- 6	- 9
$\alpha + 2$	43	- 2	4	- 8	16	11	- 22
$2\alpha^5 + 2\alpha^2 + \alpha + 1$	71	37	20	30	- 26	32	- 23
$2\alpha^5 + \alpha - 1$	113	16	30	28	- 4	49	- 7
$\alpha - 2$	127	2	4	8	16	32	- 63
$\alpha^6 - 2\alpha^3 + \alpha + 1$	197	- 6	36	- 19	- 83	- 93	- 33
$\alpha^6 - \alpha^3 - \alpha^2 - 2$	211	- 40	- 88	- 67	- 63	- 12	58

Итак, мы закончили разложение первых семи простых чисел  $\equiv 1 \pmod{7}$ . Результаты даны в табл. 4.4.2. Продолжение настоящего процесса не встречает других трудностей, кроме роста объема вычислений.

Куммер выполнил такие вычисления и нашел разложение на простые всех  $p \equiv 1 \pmod{\lambda}$  для  $\lambda \leq 19, p < 1000$ . Его результаты, опубликованные в статье 1844 г. [К6], воспроизведены в табл. 4.4.3.

Данные, приведенные в этой таблице, могут быть найдены таким же путем, каким мы выше находили разложения чисел 29 и 211 ( $\lambda = 7$ ). Разберем, например, случай  $\lambda = 13, p = 599$ . В этом случае  $p = 46\lambda + 1$ , и так как  $2^{46} \equiv 19 \pmod{599}$  (несложное вычисление), то можно положить  $k = 19$ , после чего сравнительно легко подсчитать вычеты  $k^2 \equiv -238, k^3 \equiv 270, k^4 \equiv -261, k^5 \equiv -167, k^6 \equiv -178, k^7 \equiv 212, k^8 \equiv -165, k^9 \equiv -140, k^{10} \equiv -264,$

$k^{11} \equiv -224$ ,  $k^{12} \equiv -63$ . Составление сумм и разностей  $\pm k \pm k^2 \equiv \pm 257$ ,  $\pm 219$ ;  $\pm k \pm k^3 \equiv \pm 289$ ,  $\pm 251$ , и т. д. дает  $4 \times 66$  чисел по модулю 599; среди этих чисел нет очень маленьких и нет близких к степени числа  $k$ , но есть много таких, которые отличаются друг от друга на 1, например  $k^7 - k \equiv 193$ ,  $k^2 + k^5 \equiv -405 \equiv 194$ . Это приводит к  $1 - \alpha - \alpha^2 - \alpha^5 + \alpha^7$  как к возможному делителю числа 599. Далее идет трудная часть вычисления, а именно вычисление нормы. Соответствующую работу можно минимизировать, если организовать ее следующим образом. Воспользуемся тем, что 2 является примитивным корнем по модулю 13 (приложение, § А.2), и запи-

Таблица 4.4.3

При  $\lambda=5$  и  $\alpha^\lambda = 1$ :

$11 = N(2 + \alpha)$	$461 = N(4 - \alpha - \alpha^2)$
$31 = N(2 - \alpha)$	$491 = N(5 + 3\alpha + \alpha^3)$
$41 = N(3 + 2\alpha + \alpha^3)$	$521 = N(5 + \alpha)$
$61 = N(3 + \alpha)$	$541 = N(3 - 3\alpha - \alpha^2)$
$71 = N(3 - \alpha + \alpha^2)$	$571 = N(6 + 5\alpha + 3\alpha^2)$
$101 = N(3 + \alpha - \alpha^2)$	$601 = N(5 + 2\alpha - \alpha^2)$
$131 = N(3 + \alpha - \alpha^4)$	$631 = N(4 - 2\alpha - \alpha^3)$
$151 = N(3 + 2\alpha - \alpha^4)$	$641 = N(5 + 3\alpha + 4\alpha^2)$
$181 = N(4 + 3\alpha)$	$661 = N(5 + \alpha - \alpha^2 + 3\alpha^3)$
$191 = N(4 + \alpha + 2\alpha^2)$	$691 = N(3 - 3\alpha - 2\alpha^2)$
$211 = N(3 - 2\alpha)$	$701 = N(4 - \alpha - 2\alpha^2 + \alpha^3)$
$241 = N(4 - \alpha + \alpha^2)$	$751 = N(6 + 4\alpha + 3\alpha^2)$
$251 = N(5 + 2\alpha + \alpha^4)$	$761 = N(5 - 2\alpha + \alpha^2)$
$271 = N(3 - 3\alpha + \alpha^2)$	$811 = N(3 - 3\alpha - 2\alpha^2 + \alpha^3)$
$281 = N(4 + \alpha - \alpha^2)$	$821 = N(4 - \alpha - 2\alpha^2 + 2\alpha^3)$
$311 = N(5 + 3\alpha + 2\alpha^2 + \alpha^3)$	$881 = N(6 + 2\alpha + \alpha^2)$
$331 = N(4 - 2\alpha + \alpha^2)$	$911 = N(5 + \alpha^2 - 2\alpha^4)$
$401 = N(4 + 3\alpha - \alpha^4)$	$941 = N(4 + 3\alpha - 3\alpha^2 - \alpha^3)$
$421 = N(5 + 2\alpha + 2\alpha^2)$	$971 = N(5 - 2\alpha - \alpha^4)$
$431 = N(4 - 2\alpha - \alpha^4)$	$991 = N(6 + \alpha + \alpha^3)$

При  $\lambda=7$  и  $\alpha^\lambda = 1$ :

$29 = N(1 + \alpha - \alpha^2)$	$491 = N(3 + \alpha + \alpha^3 - \alpha^5)$
$43 = N(2 + \alpha)$	$547 = N(3 + \alpha)$
$71 = N(2 + \alpha + \alpha^3)$	$617 = N(2 + \alpha + \alpha^2 - \alpha^5)$
$113 = N(2 - \alpha + \alpha^5)$	$631 = N(2 + 2\alpha - \alpha^2 + \alpha^3 + \alpha^6)$
$127 = N(2 - \alpha)$	$659 = N(2 + 2\alpha - \alpha^2 + \alpha^5)$
$197 = N(3 + \alpha + \alpha^5 + \alpha^6)$	$673 = N(4 + 3\alpha + 2\alpha^2 + \alpha^4 + 2\alpha^6)$
$211 = N(3 + \alpha + 2\alpha^2)$	$701 = N(3 + \alpha + \alpha^4 - \alpha^5 + \alpha^6)$
$239 = N(3 + 2\alpha + 2\alpha^2 + \alpha^3)$	$743 = N(3 + 2\alpha - \alpha^3 - \alpha^4)$
$281 = N(2 - \alpha - 2\alpha^3)$	$757 = N(3 + 2\alpha + \alpha^3)$
$337 = N(2 + \alpha - \alpha^2 - \alpha^4)$	$827 = N(2 + 2\alpha - \alpha^4 - \alpha^6)$

При  $\lambda = 7$  и  $\alpha^\lambda = 1$ :

$$379 = N(3 + 2\alpha + \alpha^2)$$

$$421 = N(3 + \alpha + \alpha^2)$$

$$449 = N(2 + \alpha - \alpha^3 - \alpha^6)$$

$$463 = N(3 + 2\alpha)$$

$$883 = N(2 - \alpha^2 - 2\alpha^3 - \alpha^5)$$

$$911 = N(3 + 2\alpha - \alpha^3 + \alpha^4)$$

$$953 = N(3 + \alpha - \alpha^2 - \alpha^3)$$

$$967 = N(2 + 2\alpha - \alpha^3 + 2\alpha^5)$$

При  $\lambda = 11$  и  $\alpha^\lambda = 1$ :

$$23 = N(1 + \alpha + \alpha^9)$$

$$97 = N(1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5)$$

$$89 = N(1 + \alpha + \alpha^4 + \alpha^6)$$

$$199 = N(1 + \alpha - \alpha^2)$$

$$331 = N(1 - \alpha + \alpha^3 + \alpha^5)$$

$$353 = N(1 + \alpha + \alpha^3 + \alpha^4 - \alpha^7)$$

$$397 = N(1 + \alpha + \alpha^6 - \alpha^7)$$

$$419 = N(1 + \alpha - \alpha^2 + \alpha^3)$$

$$463 = N(1 - \alpha - \alpha^2 + \alpha^5 + \alpha^6)$$

$$617 = N(2 + \alpha + \alpha^3 + \alpha^{10})$$

$$661 = N(1 + \alpha - \alpha^2 + \alpha^4 - \alpha^8)$$

$$683 = N(2 + \alpha)$$

$$727 = N(1 + \alpha + \alpha^3 - \alpha^8 - \alpha^9)$$

$$859 = N(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^7 - \alpha^8)$$

$$881 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^4 - \alpha^7 - \alpha^9)$$

$$947 = N(2 + \alpha^3 - \alpha^4 - \alpha^6)$$

$$991 = N(2 + \alpha + \alpha^3)$$

При  $\lambda = 13$  и  $\alpha^\lambda = 1$ :

$$53 = N(1 + \alpha + \alpha^3)$$

$$79 = N(1 - \alpha + \alpha^{10})$$

$$131 = N(1 - \alpha + \alpha^{11})$$

$$157 = N(1 + \alpha + \alpha^2 + \alpha^5)$$

$$313 = N(1 - \alpha + \alpha^3 + \alpha^6)$$

$$443 = N(1 + \alpha - \alpha^3 + \alpha^8)$$

$$521 = N(1 + \alpha - \alpha^{12})$$

$$547 = N(1 - \alpha - \alpha^2 + \alpha^3 + \alpha^6)$$

$$599 = N(1 + \alpha - \alpha^7 + \alpha^8 + \alpha^{11})$$

$$677 = N(1 - \alpha - \alpha^4 + \alpha^6 + \alpha^9)$$

$$859 = N(1 + \alpha - \alpha^2 - \alpha^5 + \alpha^7)^*$$

$$911 = N(1 + \alpha^3 + \alpha^5 - \alpha^7 - \alpha^{11})$$

$$937 = N(1 + \alpha^3 - \alpha^7 + \alpha^8 \rightarrow \alpha^{10})$$

При  $\lambda = 17$  и  $\alpha^\lambda = 1$ :

$$103 = N(1 + \alpha^2 + \alpha^9)$$

$$137 = N(1 + \alpha - \alpha^3)$$

$$239 = N(1 + \alpha + \alpha^3)$$

$$307 = N(1 - \alpha + \alpha^7)$$

$$409 = N(1 - \alpha^3 + \alpha^8)$$

$$443 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^{12})$$

$$613 = N(1 + \alpha^2 - \alpha^3)$$

$$647 = N(1 + \alpha + \alpha^{13} + \alpha^{15})$$

$$919 = N(1 + \alpha + \alpha^4 + \alpha^5 + \alpha^9)$$

$$953 = N(1 + \alpha + \alpha^9 - \alpha^{13})$$

При  $\lambda = 19$  и  $\alpha^\lambda = 1$ :

$$191 = N(1 + \alpha + \alpha^{16})$$

$$229 = N(1 - \alpha - \alpha^5)$$

$$419 = N(1 + \alpha - \alpha^8)$$

$$457 = N(1 + \alpha + \alpha^3)$$

$$571 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^5)$$

$$647 = N(1 - \alpha^2 + \alpha^9)$$

$$761 = N(1 - \alpha^2 + \alpha^{12})$$

\*) Здесь исправлена очевидная опечатка в таблице Куммера. Кроме того, Ленстра исправил куммерово разложение числа 599, заменив  $\alpha^{11}$  на  $-\alpha^{11}$ .

шем  $Nf(\alpha)$  в виде  $f(\alpha)f(\alpha^2)f(\alpha^4)f(\alpha^8)f(\alpha^3)f(\alpha^6)f(\alpha^{12})f(\alpha^{11})f(\alpha^9)f(\alpha^5)f(\alpha^{10}) \times \times f(\alpha^7)$ , где каждый сомножитель получается из предыдущего заменой  $\alpha$  на  $\alpha^2$ . Пусть  $g(\alpha)$  есть произведение каждого четвертого из этих 12 сомножителей, т. е.  $g(\alpha) = f(\alpha)f(\alpha^3)f(\alpha^9)$ . Тогда ясно, что  $Nf(\alpha) = g(\alpha)g(\alpha^2) \times \times g(\alpha^4)g(\alpha^8)$ . Пусть  $h(\alpha)$  есть произведение каждого второго из этих четырех сомножителей, т. е.  $h(\alpha) = g(\alpha)g(\alpha^4)$ . Тогда  $Nf(\alpha) = h(\alpha)h(\alpha^2)$ . Прямое вычисление элемента  $g(\alpha)$  не слишком длинно. В результате оказывается, что  $g(\alpha) = -3(\alpha^{12} + \alpha^{10} + \alpha^4) + 2(\alpha^{11} + \alpha^8 + \alpha^7) - 2(\alpha^9 + \alpha^3 + \alpha^1) + 6(\alpha^6 + \alpha^5 + \alpha^2) - 10$ . Пусть  $\eta_0 = \alpha + \alpha^3 + \alpha^9$ ,  $\eta_1 = \alpha^2 + \alpha^5 + \alpha^6$ ,  $\eta_2 = \alpha^4 + \alpha^{10} + \alpha^{12}$ ,  $\eta_3 = \alpha^8 + \alpha^7 + \alpha^{11}$ . Тогда замена  $\alpha$  на  $\alpha^2$  вызывает циклическую перестановку  $\eta_0 \mapsto \eta_1 \mapsto \eta_2 \mapsto \eta_3 \mapsto \eta_0$ . Таким образом,

$$h(\alpha) = g(\alpha)g(\alpha^4) = [5\eta_3 + \eta_0 + 9\eta_1 - 7][5\eta_1 + \eta_2 + 9\eta_3 - 7].$$

Для элементов  $\eta$  легко построить таблицу умножения; единственными умножениями, которые нужно действительно выполнить, являются

$$\begin{aligned}\eta_0^2 &= \alpha^2 + \alpha^4 + \alpha^{10} + \alpha^4 + \dots = \eta_1 + 2\eta_2 \\ \eta_0\eta_1 &= \eta_0 + \eta_1 + \eta_3 \\ \eta_0\eta_2 &= 3 + \eta_1 + \eta_3\end{aligned}$$

после чего другие произведения, такие, как  $\eta_0\eta_3 = \eta_3\eta_0 = \eta_{0+3} + \eta_{1+3} + \eta_{2+3} = \eta_3 + \eta_0 + \eta_2$ , могут быть получены перестановкой элементов  $\eta_i$ . Таким образом,

$$\begin{aligned}h(\alpha) &= 25\eta_1\eta_3 + 5\eta_3\eta_2 + 45\eta_3^2 - 35\eta_3 + 5\eta_0\eta_1 + \eta_0\eta_2 + 9\eta_0\eta_3 - 7\eta_0 + \\ &\quad + 45\eta_1^2 + 9\eta_1\eta_2 + 81\eta_1\eta_3 - 63\eta_1 - 35\eta_1 - 7\eta_2 - 63\eta_3 + 49 = \\ &= 49 - 7\eta_0 - 98\eta_1 - 7\eta_2 - 98\eta_3 + 25(3 + \eta_2 + \eta_0) + \\ &\quad + 5(\eta_2 + \eta_3 + \eta_1) + 45(\eta_0 + 2\eta_1) + 5(\eta_0 + \eta_1 + \eta_3) + \\ &\quad + (3 + \eta_1 + \eta_3) + 9(\eta_3 + \eta_0 + \eta_2) + 45(\eta_2 + 2\eta_3) + \\ &\quad + 9(\eta_1 + \eta_2 + \eta_0) + 81(3 + \eta_2 + \eta_0) = \\ &= 370 + 167\eta_0 + 12\eta_1 + 167\eta_2 + 12\eta_3 = \\ &= 370 + 167\theta_0 + 12\theta_1 = 358 + 155\theta_0\end{aligned}$$

где  $\theta_0 = \eta_0 + \eta_2 = \alpha + \alpha^4 + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^{10}$  и  $\theta_1 = \eta_1 + \eta_3 = \alpha^2 + \alpha^8 + \alpha^6 + \alpha^{11} + \alpha^5 + \alpha^7 = -1 - \theta_0$ . Далее,  $\theta_0\theta_1 = 3\theta_0 + 3\theta_1 = -3$ ,  $h(\alpha^2) = 358 + 155\theta_1$ , и наконец  $Nf(\alpha) = (358 + 155\theta_0)(358 + 155\theta_1) = 358^2 + 358 \cdot 155(\theta_0 + \theta_1) - 3 \cdot 155^2 = 128\,164 - 55\,490 - 72\,075 = 599$ , что и требовалось. Таким образом,  $1 - \alpha - \alpha^2 - \alpha^5 + \alpha^7$  есть простой делитель числа 599. (Куммер в этом случае ошибся. См. упр. 8.)

В заключение рассмотрим случай  $\lambda = 23$ . Первое простое  $p \equiv 1 \pmod{23}$  есть  $p = 47$ . В этом случае  $k$  может быть взято любым квадратом по модулю 47, например  $k = 4$ . Тогда степени  $k, k^2, k^3, \dots$  по модулю 47 легко находятся: 4, 16, 17, 21, -10, 7, -19, 18, -22, 6, 24, 2, 8, -15, -13, -5, -20,

14, 9,  $-11$ , 3, 12 (в таком порядке). Разумеется,  $k^{23} \equiv 1 \pmod{23}$ . Очевидным подозреваемым на роль делителя числа 47, который делит  $\alpha - 4$ , будет  $1 - \alpha + \alpha^{21}$ , поскольку  $1 - 4 + 3 = 0$ . Для того чтобы следовать используемой выше процедуре, необходимо вычислить  $N(1 - \alpha + \alpha^{21})$ . Так как  $22 = 11 \cdot 2$ , то это вычисление можно свести к перемножению 11 сомножителей, а затем перемножению двух сомножителей. Примитивный корень по модулю 23 есть  $-2$ , так что указанное сведение имеет следующий вид:  $Nf(\alpha) = G(\alpha)G(\alpha^{-2})$ , где

$$G(\alpha) = f(\alpha)f(\alpha^4)f(\alpha^{-7})f(\alpha^{-5})f(\alpha^3)f(\alpha^{-11})f(\alpha^2)f(\alpha^8)f(\alpha^9)f(\alpha^{-10})f(\alpha^6).$$

(Здесь  $\alpha^{-2}$  означает  $\alpha^{21}$ ,  $\alpha^{-7}$  означает  $\alpha^{16}$ , и т. д.) Вычисление элемента  $G(\alpha)$  довольно длинное. Его можно организовать следующим образом. Пусть  $g(\alpha) = f(\alpha)f(\alpha^4)$  и  $h(\alpha) = g(\alpha)f(\alpha^{-7})$ , так что  $G(\alpha) = h(\alpha)h(\alpha^{-5})h(\alpha^2) \times \times g(\alpha^{-10})$ . Тогда

$$g(\alpha) = \alpha^{21} - \alpha^{16} + \alpha^{15} + \alpha^{13} + \alpha^5 - \alpha^4 - \alpha^2 - \alpha + 1$$

$$h(\alpha) = \alpha^{20} + \alpha^{19} + \alpha^{17} - 3\alpha^{16} + \alpha^{13} + \alpha^{12} + \alpha^9 - \alpha^8 - \alpha^7 + \alpha^5 - \alpha^2 - \alpha + 1$$

$$h(\alpha^{-5}) = \alpha^{15} + \alpha^{20} + \alpha^7 - 3\alpha^{12} + \alpha^4 + \alpha^9 + \alpha - \alpha^6 - \alpha^{11} + \alpha^{21} - \alpha^{13} - \alpha^{18} + 1$$

$$h(\alpha^2) = \alpha^{17} + \alpha^{15} + \alpha^{11} - 3\alpha^9 + \alpha^3 + \alpha + \alpha^{18} - \alpha^{16} - \alpha^{14} + \alpha^{10} - \alpha^4 - \alpha^2 + 1$$

$$g(\alpha^{-10}) = \alpha^{20} - \alpha + \alpha^{11} + \alpha^8 + \alpha^{19} - \alpha^6 - \alpha^3 - \alpha^{13} + 1$$

и вычисление элемента  $G(\alpha)$  требует двух умножений средней сложности, сопровождаемых довольно длинным перемножением двух их результатов. Окончательно, получаем  $G(\alpha) = -44 + 15\theta_0 - 13\theta_1$ , где  $\theta_0 = \alpha + \alpha^4 + \alpha^{-7} + \dots + \alpha^6$  и  $\theta_1 = -1 - \theta_0$ . Поскольку  $\theta_0\theta_1$ , как легко убедиться простым перемножением, есть  $11 + 5\theta_0 + 5\theta_1 = 6$ , то это дает  $G(\alpha)G(\alpha^{-2}) = (-31 + 28\theta_0)(-31 + 28\theta_1) = 31^2 - 31 \cdot 28(\theta_0 + \theta_1) + 6 \cdot 28^2 = 961 + 868 + 4704 = 6533 = 47 \cdot 139$ . Таким образом, наша процедура этой попыткой не дала нам делителя числа 47. На самом деле легко видеть, что она *никогда* не может дать такого делителя, поскольку, каким бы ни был исходный элемент  $f(\alpha)$ , построенный для него аналог элемента  $G(\alpha)$  может быть представлен в виде  $a + b\theta_0$ , так что требуемый результат должен иметь вид  $47 = (a + b\theta_0)(a + b\theta_1) = a^2 - ab + 6b^2$ . Невозможность такого равенства может быть доказана применением гауссовой теории бинарных квадратичных форм, или, проще, если записать это равенство в виде  $4 \cdot 47 = 4a^2 - 4ab + 24b^2$ ,  $188 = (2a - b)^2 + 23b^2$ . Лишь два испытания необходимы, чтобы проверить невозможность представления числа 188 в виде суммы квадрата и еще квадрата, умноженного на 23 ( $188 - 23$  и  $188 - 23 \cdot 4$  не являются квадратами).

Это доказывает, что в случае  $\lambda = 23$  нет круговых целых с нормой 47. Так как  $N(\alpha - 4) \equiv 0 \pmod{47}$ , то простой делитель числа 47 должен был бы делить одно из сопряженных числа  $\alpha - 4$  и, следовательно, по теореме предыдущего параграфа, должен был бы иметь нормой 47. Таким образом, 47 *совсем не имеет простых делителей*, и уж тем более здесь не может быть единственности разложения. Эту аномалию можно обнаружить и более простым способом, не обращаясь к теореме предыдущего параграфа. Так как  $1 - \alpha + \alpha^{-2}$  делит  $47 \cdot 139$ , но не делит ни одно из чисел 47 и 139 (поскольку его норма не делит ни  $N(47) = 47^{22}$ , ни  $N(139) = 139^{22}$ ), то оно не является простым, и если бы выполнялись обычные свойства разложения, то оно развалилось бы на 2 сомножителя. Но так как его норма равна  $47 \cdot 139$ , то един-

ственным возможным разложением было бы разложение на множитель с нормой 47 и множитель с нормой 139, а как мы только что видели, число 47 не является нормой. [Ситуация здесь в точности такая же, как в упомянутом выше примере нарушения единственности разложения  $3 \cdot 7 = N(4 + \sqrt{-5})$  для квадратичных целых  $x + y\sqrt{-5}$ . Так как  $4 + \sqrt{-5}$  делит  $3 \cdot 7$ , но не делит ни 3, ни 7 (поскольку его норма не делит ни  $N(3) = 3^2$ , ни  $N(7) = 7^2$ ), оно не является простым и должно быть произведением множителя с нормой 3 и множителя с нормой 7. Но равенство  $N(x + y\sqrt{-5}) = x^2 + 5y^2 = 3$  невозможно.]

Из восьми простых  $p \equiv 1 \pmod{23}$ , меньших 1000, Куммер для трех дал решение  $h(\alpha)$  уравнения  $Nh(\alpha) \equiv p$  (табл. 4.4.4.), а для остальных пяти,

Таблица 4.4.4

$\lambda = 23 \quad \text{и} \quad \alpha^\lambda = 1$
$599 = N(1 + \alpha^{15} - \alpha^{16})$
$691 = N(1 + \alpha + \alpha^5)$
$829 = N(1 + \alpha^{11} + \alpha^{20})$

включая  $p = 47$  и  $p = 139$ , показал приведенными выше рассуждениями, что такого  $h(\alpha)$  не существует. Для каждого из пяти этих  $p$  он дал такое круговое целое  $h(\alpha)$ , что  $h(\alpha^{-1}) = h(\alpha)$  и произведение 11 сопряженных числа  $h(\alpha)$ , получаемых заменой  $\alpha \mapsto \alpha^4$ , равно  $p$ . (Иначе говоря,

$$p = h(\alpha)h(\alpha^4)h(\alpha^{-7})h(\alpha^{-5})h(\alpha^3)h(\alpha^{-11})h(\alpha^2)h(\alpha^8)h(\alpha^9)h(\alpha^{-10})h(\alpha^6).$$

Тогда, поскольку  $h(\alpha) = h(\alpha^{-1})$ ,  $Nh(\alpha) = p^2$ .) Эти 5 круговых целых даны в табл. 4.4.5. Здесь четко прослеживаются два совершенно различных пути

Таблица 4.4.5

$\lambda = 23 \quad \text{и} \quad \alpha^\lambda = 1$
$47^2 = N(\alpha^{10} + \alpha^{-10} + \alpha^8 + \alpha^{-8} + \alpha^7 + \alpha^{-7})$
$139^2 = N(\alpha^{10} + \alpha^{-10} + \alpha^8 + \alpha^{-8} + \alpha^4 + \alpha^{-4})$
$277^2 = N(2 + \alpha + \alpha^{-1} + \alpha^7 + \alpha^{-7})$
$461^2 = N(\alpha + \alpha^{-1} + \alpha^{10} + \alpha^{-10} + \alpha^8 + \alpha^{-8} + \alpha^9 + \alpha^{-9})$
$967^2 = N(2 + \alpha^{11} + \alpha^{-11} + \alpha^4 + \alpha^{-4})$

разложения числа  $47 \cdot 139$ : одно в виде  $N(1 - \alpha + \alpha^{-2})$ , а другое в виде произведения куммерова разложения числа 47 на его разложение числа 139. В первом разложении 22 сомножителя и норма каждого из них равна  $47 \cdot 139$ , а во втором 11 сомножителей с нормой  $47^2$  и 11 сомножителей с нормой  $139^2$ . Все эти сомножители неразложимы, поскольку числа 47 и 139 не могут быть нормами.



Ядром куммеровской теории идеальных комплексных чисел является то простое соображение, что способ проверки делимости на гипотетический множитель числа 47, а именно, проверки сравнения  $g(4) \equiv 0 \pmod{47}$ , применим даже тогда, когда нет никакого реального множителя, для которого проводится проверка. Можно рассматривать это как проверку делимости на некий *идеальный* делитель числа 47, и в этом суть куммеровской теории. Однако прежде чем Куммер смог сделать этот решительный шаг, ему пришлось мастерски овладеть разложением простых  $p \not\equiv 0, 1 \pmod{\lambda}$ , и именно этим он и занялся в период с 1844 до 1846 г. Здесь он тоже нашел методы проверки делимости на простые делители числа  $p$ , которые продолжали действовать даже тогда, когда не было никаких реальных делителей, для которых должна была проводиться проверка. Он по определению рассматривал их как признаки делимости на «идеальные простые делители» числа  $p$  и построил свою теорию идеальных комплексных чисел на основе этих идеальных простых делителей.

Следующие четыре параграфа посвящены изучению простых делителей простых чисел  $p \not\equiv 0, 1 \pmod{\lambda}$ , обобщающему изложенное выше исследование случая  $p \equiv 1 \pmod{\lambda}$ . Накопленный в них опыт используется затем для того, чтобы обосновать очень естественное определение *идеальных простых делителей*, которые в этой книге будут называться *простыми дивизорами*.

## Упражнения

- Проверьте следующие вычисления ( $\lambda = 5$ ).
  - $(3 - \alpha)(2 + \alpha)(2 + \alpha^3)(2 + \alpha^4) = 11(\alpha^4 + \alpha^3 + 2)$ .
  - $(2 + \alpha^2)^2$  делит  $3 - \alpha$ , и частное есть единица. Найдите эту единицу и обратную к ней.
  - $(2 + \alpha^2)(3\alpha^4 + 2\alpha^2 + 1)$  делит  $5 + 2\alpha$ , и частное есть единица.
  - $2 + \alpha$  делит  $5 - 4\alpha^2$ . Какова норма частного?
  - $2\alpha^3 + \alpha^4 + 4$ ,  $2\alpha^2 + \alpha + 4$  и  $2\alpha + \alpha^3 + 4$  не делятся на  $2\alpha^4 + \alpha^2 + 4$ .
  - $(\alpha^3 + 2)(2\alpha^3 + \alpha^4 + 4)$  делит  $\alpha + 7$ , и частное есть единица.
  - $\alpha + 2$  делит  $\alpha^4 - 5$ .
- Проверьте следующие утверждения в случае  $\lambda = 7$ .
  - $2\alpha^5 + 2\alpha^2 + \alpha + 1$  имеет норму 71 и делит  $3 - 2\alpha$ .
  - $4 + \alpha$  делится на одно из сопряженных числа  $1 + \alpha^2 - \alpha^4$ . Найдите частное.
  - $N(2 + 2\alpha^2 + \alpha^6) = 197$ .
  - $N(3 - \alpha^4 - \alpha^6) = 8 \cdot 197$ .
  - Найдите элемент с нормой 8. Заметим, что не все простые делители нормы обязаны быть сравнимы с 1 по модулю 7.
- Разложите следующие круговые целые ( $\lambda = 5$ ).
  - $5\alpha^4 - 3\alpha^3 - 5\alpha^2 + 5\alpha - 2$ .
  - $-4\alpha^3 - 11\alpha^2 + 8\alpha + 15$ .
- При  $\lambda = 7$  разложите (a)  $\alpha^2 - 3\alpha - 4$ , (b)  $\alpha^5 - \alpha^4 - 3\alpha^2 - 3\alpha - 2$ .
- В случае  $\lambda = 7$ ,  $p = 71$  делитель в куммеровской таблице заметно отличается от найденного в тексте. Запишите один из них как единицу, умноженную на элемент, сопряженный другому.
- Найдите элемент с нормой  $p$  в случае  $\lambda = 19$ ,  $p = 191$ . Сравните ответ с куммеровым в табл. 4.4.3.
- Как и в упр. 6, постройте другие данные из куммеровской таблицы.
- Покажите, что куммеров делитель в случае  $\lambda = 13$ ,  $p = 599$  ошибочен. [Он не удовлетворяет условию  $f(k) \equiv 0 \pmod{p}$  при некотором  $k$ .]
- Пусть  $\lambda = 23$ . Условие  $f(\alpha^{-1}) = f(\alpha)$  в сочетании с  $f(4) \equiv 0 \pmod{47}$  дает условие вида  $a_0 + 16a_1 + \dots - 21a_{11} \equiv 0 \pmod{47}$  на 12 переменных  $a_0, a_1, \dots, a_{11}$ . Отыщите несколько несложных кандидатов на решения

уравнений  $Nf(\alpha) = 47^2$ ,  $f(\alpha) = f(\alpha^{-1})$ . Покажите, что сопряженное куммерову делителю  $\alpha^{10} + \alpha^{13} + \alpha^8 + \alpha^{15} + \alpha^7 + \alpha^{16}$  удовлетворяет этому условию. Подсчитайте  $Nf(\alpha)$  для этого кандидата.

10. Докажите, что если  $\lambda$  делит  $Ng(\alpha)$ , то  $\alpha - 1$  делит  $g(\alpha)$ .

11. Докажите, что  $(\alpha^2 - 1)(\alpha^3 - 1) \dots (\alpha^{\lambda-1} - 1) = 1 + 2\alpha + 3\alpha^2 + \dots + \lambda\alpha^{\lambda-1} = \alpha + 2\alpha^2 + \dots + (\lambda - 1)\alpha^{\lambda-1}$ .

## 4.5. Периоды

В вычислениях предыдущего параграфа оказалось полезным выбрать примитивный корень  $\gamma$  по модулю  $\lambda$  и записывать сомножители нормы  $Ng(\alpha)$  кругового целого  $g(\alpha)$  в порядке  $Ng(\alpha) = g(\alpha)g(\alpha^\gamma)g(\alpha^{\gamma^2}) \dots$ , а не в порядке  $Ng(\alpha) = g(\alpha)g(\alpha^2) \times \dots$ . Во избежание показателей в показателях удобно ввести обозначение для сопряжения  $\alpha \mapsto \alpha^\gamma$ , например через  $\sigma$ . Тогда  $\sigma g(\alpha) = g(\alpha^\gamma)$ ,  $\sigma^2 g(\alpha) = g(\alpha^{\gamma^2})$  и т. д., и  $Ng(\alpha) = g(\alpha) \cdot \sigma g(\alpha) \cdot \sigma^2 g(\alpha) \dots \sigma^{\lambda-2} g(\alpha)$ . Заметим, что  $\sigma^{\lambda-1}$  есть тождественное сопряжение  $\alpha \mapsto \alpha$  и что сопряжения  $\sigma, \sigma^2, \dots, \sigma^{\lambda-1}$  все различны, поскольку они переводят  $\alpha$  в различные степени числа  $\alpha$ .

Метод, примененный в предыдущем параграфе к вычислению нормы, заключался в том, что при помощи делителя  $e$  числа  $\lambda - 1$  норма записывалась в виде  $Ng(\alpha) = G(\alpha) \cdot \sigma G(\alpha) \dots \sigma^{e-1} G(\alpha)$ , где <sup>1)</sup>  $G(\alpha) = g(\alpha) \cdot \sigma^e g(\alpha) \cdot \sigma^{2e} g(\alpha) \dots \sigma^{-e} g(\alpha)$ . Этим путем можно сократить число умножений, нужных для нахождения  $Ng(\alpha)$ . Например, в случае  $\lambda = 13$  использовался примитивный корень  $\gamma = 2$  при  $e = 4$ , чтобы записать  $Ng(\alpha) = G(\alpha) G(\alpha^2) \times \dots \times G(\alpha^4) G(\alpha^8)$ , где  $G(\alpha) = g(\alpha) g(\alpha^3) g(\alpha^9)$ . Кроме того, тот факт, что  $\sigma^e G(\alpha) = G(\alpha)$  (сопряжения  $\sigma^e$  лишь переставляет сомножители в  $G(\alpha)$ ), означает, что  $G(\alpha)$  имеет очень специальный вид. В примере при  $\lambda = 13$ ,  $\gamma = 2$ ,  $e = 4$  этот элемент имел вид  $a + b\eta_0 + c\eta_1 + d\eta_2$ , где  $\eta_0 = \alpha + \alpha^3 + \alpha^9$ ,  $\eta_1 = \alpha^2 + \alpha^6 + \alpha^5$ ,  $\eta_2 = \alpha^4 + \alpha^{12} + \alpha^{10}$  и  $\eta_3 = \alpha^8 + \alpha^{11} + \alpha^7$ . Таким же образом, в общем случае  $G(\alpha)$  имеет вид  $a + b\eta_0 + c\eta_1 + \dots + d\eta_{e-1}$ , где  $a, b, c, \dots, d$  — целые числа,  $\eta_0 = \alpha + \sigma^e \alpha + \sigma^{2e} \alpha + \dots + \sigma^{-e} \alpha$  и  $\eta_{i+1} = \sigma \eta_i$ . Это следует из того, что в силу равенства  $\sigma^e G(\alpha) = G(\alpha)$  коэффициент при  $\alpha$  в  $G(\alpha)$  равен коэффициенту при  $\sigma^e \alpha$  и, вообще, коэффициент при  $\alpha^j$  равен коэффициенту при  $\sigma^e \alpha^j$ . Круговые целые  $\eta_0, \eta_1, \dots, \eta_{e-1}$ , определенные таким способом для данных  $\lambda, \gamma, e$ , называются *периодами*; это название дал им Гаусс в седьмом разделе своих «Арифметических исследований» (*Disquisitiones Arithmeticae*, Art. 343). Периоды играют важную роль не только в том, довольно мелком, приложении, которое приведено в предыдущем параграфе, но и в широком круге других приложений в теории чисел и линейной алгебре, и использование их Гауссом в исследованиях, относящихся к построению правильных многоугольников, было лишь первым

<sup>1)</sup> Здесь  $\sigma^{-e}$  обозначает  $\sigma^{\lambda-1-e}$ , т. е. сопряжение, обратное к  $\sigma^e$ .

примером таких приложений. Куммер хорошо знал о том, что Гаусс пользовался периодами, и сам широко применял их, развивая теорию разложения круговых целых.

Пусть  $\lambda$ ,  $\gamma$ ,  $e$  те же, что и раньше (т. е.  $\lambda$  — нечетное простое число,  $\gamma$  — примитивный корень по модулю  $\lambda$  и  $e$  — делитель числа  $\lambda - 1$ ). Пусть  $f = (\lambda - 1)/e$ . Тогда  $\eta_0 = \alpha + \sigma^e \alpha + \sigma^{2e} \alpha + \dots + \sigma^{-e} \alpha$  содержит  $f$  слагаемых, поскольку  $\sigma^{ef} \alpha = \sigma^{\lambda-1} \alpha = \alpha$ ,  $\sigma^{-e} \alpha = (\sigma^e)^{f-1} \alpha$ . Значит,  $\eta_0, \eta_1, \dots, \eta_{e-1}$  все состоят из  $f$  слагаемых. По этой причине они называются *периодами длины  $f$* . Заметим, что естественно определить  $\eta_0 = \eta_e$  (поскольку  $\eta_e$  должно было бы равняться  $\sigma \eta_{e-1} = \sigma^2 \eta_{e-2} = \dots = \sigma^e \eta_0 = \eta_0$ ) и  $\eta_1 = \eta_{e+1}, \eta_2 = \eta_{e+2}, \dots$ , а также  $\eta_{-1} = \eta_{e-1}, \eta_{-2} = \eta_{e-2}, \dots$ , чтобы  $\eta_i$  было определено для всех целых  $i$  и  $\sigma \eta_i = \eta_{i+1}$ . Для данного  $\lambda$  и для данного  $f$ , которое делит  $\lambda - 1$ , периоды длины  $f$  определяются в зависимости от выбора примитивного корня  $\gamma$ . (Полагаем  $\sigma(\alpha) = \alpha^\gamma$  и  $e = (\lambda - 1)/f$  в формулах, определяющих периоды.) Однако вполне законно говорить о «периодах длины  $f$ », поскольку сами периоды не зависят от выбора примитивного корня  $\gamma$ , хотя их порядок и может от него зависеть. В этом можно убедиться следующим образом.

Пусть  $\gamma'$  — другой примитивный корень по модулю  $\lambda$ , пусть  $\sigma'$  обозначает соответствующее сопряжение  $\alpha \mapsto \alpha^{\gamma'}$ , и пусть  $\eta'_i$  — периоды длины  $f$ , определенные при помощи  $\sigma'$  вместо  $\sigma$ . Для того чтобы доказать, что периоды  $\eta_1, \eta_2, \dots, \eta_e$  совпадают, вообще говоря, с точностью до порядка, с периодами  $\eta'_1, \eta'_2, \dots, \eta'_e$ , необходимо и достаточно показать, что если  $\alpha^j$  есть некоторая степень числа  $\alpha$ , а  $\eta_i$  есть тот период, который ее содержит, то  $\eta_i$  содержит также и  $\sigma'^e \alpha^j$ . (Тогда он также содержит  $\sigma'^e \sigma'^e \alpha^j = \sigma'^{2e} \alpha^j, \sigma'^{3e} \alpha^j, \dots, \sigma'^{-e} \alpha^j$ , т. е. все слагаемые периода  $\eta'_k$ , содержащего  $\alpha^j$ .) Для этого достаточно доказать, что  $\sigma'^e$  есть некоторая степень сопряжения  $\sigma^e$ . Но так как каждое сопряжение есть степень сопряжения  $\sigma$  (каждое отличное от нуля по модулю  $\lambda$  целое число сравнимо со степенью числа  $\gamma$ ), то и  $\sigma'$  есть степень сопряжения  $\sigma$ , а отсюда сразу вытекает, что  $\sigma'^e$  есть степень сопряжения  $\sigma^e$ . Это доказывает, что периоды  $\eta$  совпадают с периодами  $\eta'$ . Чтобы показать, что порядок может быть другим, достаточно найти соответствующий пример. Таким примером является случай  $\lambda = 13, f = 3$ . Примитивные корни по модулю 13 суть  $\pm 2, \pm 6$ . При  $\gamma = 2$  периоды длины 3 таковы:

$$\eta_1 = \alpha^2 + \alpha^6 + \alpha^5$$

$$\eta_2 = \alpha^4 + \alpha^{-1} + \alpha^{-3}$$

$$\eta_3 = \alpha^{-5} + \alpha^{-2} + \alpha^{-6}$$

$$\eta_0 = \eta_4 = \alpha^3 + \alpha^{-4} + \alpha.$$

(Заметим, что столбцы в правых частях, прочитанные сверху вниз и при переходе к столбцам слева направо, состоят в точности из степеней  $\alpha^2, \alpha^4, \alpha^8 = \alpha^{-5}, \alpha^{16} = \alpha^3, \alpha^{32} = \alpha^6, \dots$  элемента  $\alpha$  в том порядке, который предписывается выбранным примитивным корнем 2.) При  $\gamma' = -2$  период  $\eta'_1$  должен содержать  $\alpha^{-2}$  и, значит,  $\eta'_1 = \eta_3 \neq \eta_1$ .

Говорят, что круговое целое образовано периодами длины  $f$ , если оно имеет вид  $a_0 + a_1\eta_1 + a_2\eta_2 + \dots + a_e\eta_e$ , где  $a_0, a_1, \dots, a_e$  — целые числа, а  $\eta_1, \eta_2, \dots, \eta_e$  — периоды длины  $f$ . Как уже отмечалось,  $G(\alpha)$  образовано периодами длины  $f$  тогда и только тогда, когда  $\sigma^e G(\alpha) = G(\alpha)$ . Отсюда вытекает (поскольку  $\sigma^e$  есть сопряжение и потому переводит произведение в произведение), что произведение двух круговых целых, образованных периодами, само образовано периодами.

Например, для периодов  $\eta_0, \eta_1, \eta_2, \eta_3$  длины 3 при  $\lambda = 13$  таблица умножения

$$\begin{aligned}\eta_0^2 &= \eta_1 + 2\eta_2 \\ \eta_0\eta_1 &= \eta_0 + \eta_1 + \eta_3 \\ \eta_0\eta_2 &= 3 + \eta_1 + \eta_3\end{aligned}$$

была найдена в предыдущем параграфе. Применение сопряжения  $\sigma$  к этим равенствам дает  $\eta_1^2 = \eta_2 + 2\eta_3, \eta_2^2 = \eta_3 + 2\eta_0, \eta_3^2 = \eta_0 + 2\eta_1, \eta_1\eta_2 = \eta_1 + \eta_2 + \eta_0$  и т. д.

Заметим, что в некоторых местах мы пользовались записью  $\eta_0$ , а в других — записью  $\eta_e$ . Куммер постоянно пользовался обозначением  $\eta_0$  и записывал в общем случае круговое целое, образованное периодами, в виде  $a_0\eta_0 + a_1\eta_1 + \dots + a_{e-1}\eta_{e-1}$ , применяя для исключения целых чисел из этого выражения тождество  $1 + \eta_0 + \eta_1 + \dots + \eta_{e-1} = 0$ . В некоторых местах этой книги мы будем следовать обозначениям Куммера, но иногда для круговых целых, образованных периодами длины  $f = (\lambda - 1)/e$ , удобнее будет применять запись  $a_0 + a_1\eta_1 + a_2\eta_2 + \dots + a_e\eta_e$ .

## Упражнения

1. В случае  $\lambda = 5$  найдите периоды длины 2 и таблицу умножения для них. Найдите формулу для нормы кругового целого, образованного периодами длины 2 ( $\lambda = 5$ ). Найдите круговое целое, норма которого делится на простое число, не сравнимое ни с 1, ни с 0 по модулю 5. Заметим отсюда, что если это круговое целое имеет простой делитель, то он не относится к тому типу, который изучался в предыдущем параграфе.

2. Покажите, что если  $\lambda = 7$ , то норма любого кругового целого имеет вид  $[A^2 + 7B^2]/4$ , где  $A$  и  $B$  — целые числа одинаковой четности. [Пусть  $\theta_0, \theta_1$  — периоды длины 3. Найдите  $\theta_0\theta_1$ .]

3. Найдите общую формулу для  $(\theta_0 - \theta_1)^2$ , где  $\theta_0, \theta_1$  — периоды длины  $(\lambda - 1)/2$ , индуктивно, т. е. вычисляя это целое число для различных значений  $\lambda$ .

4. Докажите формулу, найденную в упр. 3.

5. Для всех случаев имеется формула для  $Ng(\alpha)$ , аналогичная формуле  $Ng(\alpha) = [A^2 + 7B^2]/4$  в случае  $\lambda = 7$ . Найдите эту формулу.

6. Найдите периоды и таблицу умножения для них в случае  $\lambda = 17$ ,  $f = 4$ .

7. Какие условия нужно наложить на  $p$  и  $f$ , чтобы периоды длины  $f$  были инвариантны при сопряжении  $\alpha \mapsto \alpha^p$ , где  $p$  — простое.

8. Покажите, что для данных  $f$  и  $\lambda$  ( $\lambda$  — простое,  $f \mid (\lambda - 1)$ ) период  $\eta_0$  не зависит от выбора примитивного корня  $\gamma$ .

## 4.6. Разложение простых $p \not\equiv 1 \pmod{\lambda}$

Пусть  $h(\alpha)$  — некоторое простое круговое целое (для данного фиксированного  $\lambda$ ). Рассуждения, содержащиеся в § 4.3, позволяют показать, что имеется простое целое число  $p$ , обладающее таким свойством:  $h(\alpha)$  делит целое число  $u$  тогда и только тогда, когда  $u \equiv 0 \pmod{p}$ ; иными словами, сравнение  $u \equiv v \pmod{h(\alpha)}$  для целых чисел  $u$  и  $v$  эквивалентно сравнению  $u \equiv v \pmod{p}$ . Для этого достаточно заметить, что  $h(\alpha)$  делит целое число  $Nh(\alpha)$  и, следовательно, делит по крайней мере один из простых целых делителей числа  $Nh(\alpha)$ , например  $h(\alpha) \mid p$ . Тогда для произвольно взятого целого числа  $u$  из  $h(\alpha) \mid u$  вытекает, что  $h(\alpha)$  делит наибольший общий делитель  $d$  чисел  $u$  и  $p$ , поскольку  $d = ap + bu$ ; с другой стороны,  $p$  — простое, так что  $d = 1$  или  $p$ , и так как  $h(\alpha)$  не единица, то  $d \neq 1$ ,  $d = p$ ,  $u \equiv 0 \pmod{p}$ . Конечно, верно и обратное: из  $u \equiv 0 \pmod{p}$  вытекает  $u \equiv 0 \pmod{h(\alpha)}$ ; таким образом, два утверждения эквивалентны.

В случае простых делителей  $h(\alpha)$ , изученных в § 4.3, этот факт мог бы служить основой признака делимости на  $h(\alpha)$ , поскольку для таких делителей каждое круговое целое сравнимо по модулю  $h(\alpha)$  с обычным целым числом. Однако это применимо *только* к тем простым  $h(\alpha)$ , которые делят простые целые числа  $p \equiv 0$  или  $1 \pmod{\lambda}$ , поэтому нужны и другие методы нахождения простых делителей  $h(\alpha)$  простых целых чисел  $p \not\equiv 0$  и  $1 \pmod{\lambda}$ .

Полезно задать вопрос: для данного простого  $h(\alpha)$ , делящего  $p$ , *какие* круговые целые  $g(\alpha)$  сравнимы с целыми числами по модулю  $h(\alpha)$ ? Необходимое условие для сравнения  $g(\alpha) \equiv u \pmod{h(\alpha)}$  непосредственно следует из теоремы Ферма  $u^p \equiv u \pmod{p}$ , поскольку это дает  $g(\alpha)^p \equiv u^p \equiv u \equiv g(\alpha) \pmod{h(\alpha)}$ . Проверить выполнение этого необходимого условия очень помогает сравнение

$$g(\alpha)^p \equiv g(\alpha^p) \pmod{p},$$

которое представляет собой не что иное, как обобщение теоремы Ферма. Его можно доказать следующим образом.

Рассмотрим  $(X + Y)^p - X^p - Y^p$  как полином от двух переменных с целыми коэффициентами. Каждое слагаемое имеет степень  $p$  и нет слагаемых с  $X^p$  и  $Y^p$ , так что полином имеет вид  $c_1 X^{p-1} Y + c_2 X^{p-2} Y^2 + \dots + c_{p-1} X Y^{p-1}$ , где  $c_i$  — положительные целые числа. Если  $Y = 1$ , а  $X$  равен целому числу, скажем  $X = u$ , то значение полинома равно, с одной стороны,  $c_1 u^{p-1} + c_2 u^{p-2} + \dots + c_{p-1} u$ , а с другой стороны,  $(u + 1)^p - u^p - 1^p \equiv (u + 1) - u - 1 = 0 \pmod{p}$ . В силу рассуждения Эйлера с разностями из § 2.4, единственным случаем, когда все значения полинома степени меньше  $p$  при целых значениях переменной сравнимы с нулем по модулю  $p$ , является такой случай, когда все его коэффициенты  $\equiv 0 \pmod{p}$ ; таким образом <sup>1)</sup>,  $c_1 \equiv c_2 \equiv \dots \equiv c_{p-1} \equiv 0 \pmod{p}$ . Значит, для любых двух круговых целых  $g_0(\alpha)$ ,  $g_1(\alpha)$  мы получаем  $(g_0(\alpha) + g_1(\alpha))^p - g_0(\alpha)^p - g_1(\alpha)^p = c_1 g_0(\alpha)^{p-1} g_1(\alpha) + \dots + c_{p-1} g_0(\alpha) g_1(\alpha)^{p-1} \equiv 0 \pmod{p}$ , и, следовательно,

$$(g_0(\alpha) + g_1(\alpha))^p \equiv g_0(\alpha)^p + g_1(\alpha)^p \pmod{p}.$$

Поэтому если  $g(\alpha) = a_0 + a_1 \alpha + \dots + a_{\lambda-1} \alpha^{\lambda-1}$ , то  $g(\alpha)^p \equiv a_0^p + (a_1 \alpha + a_2 \alpha^2 + \dots + a_{\lambda-1} \alpha^{\lambda-1})^p \equiv a_0^p + a_1^p \alpha^p + (a_2 \alpha^2 + \dots + a_{\lambda-1} \alpha^{\lambda-1})^p \equiv \dots \equiv a_0^p + a_1^p \alpha^p + a_2^p \alpha^{2p} + \dots + a_{\lambda-1}^p \alpha^{(\lambda-1)p} \pmod{p}$ . Так как  $a_i^p \equiv a_i \pmod{p}$ , то  $g(\alpha)^p \equiv g(\alpha^p) \pmod{p}$ , что и требовалось доказать.

Таким образом,  $g(\alpha)^p \equiv g(\alpha^p) \pmod{h(\alpha)}$  и необходимым условием для  $g(\alpha) \equiv u \pmod{h(\alpha)}$  является  $g(\alpha^p) \equiv g(\alpha) \pmod{h(\alpha)}$ . Наиболее простой путь нахождения круговых целых, удовлетворяющих этому условию, дает рассмотрение тех круговых целых  $g(\alpha)$ , для которых  $g(\alpha^p)$  равно самому  $g(\alpha)$ , т. е. круговых целых, инвариантных относительно сопряжения  $\alpha \mapsto \alpha^p$ . Необходимые и достаточные условия равенства  $g(\alpha) = g(\alpha^p)$  легко вывести, например, следующим образом. Пусть  $\tau$  обозначает сопряжение  $\alpha \mapsto \alpha^p$ , и пусть  $f$  — наименьшее положительное целое число, для которого  $\tau^f$  есть тождественное сопряжение  $\alpha \mapsto \alpha$ ; иными словами, пусть  $f$  — наименьшее поло-

<sup>1)</sup> Иными словами, биномиальные коэффициенты  $\binom{p}{j}$  делятся на  $p$  при  $j = 1, 2, \dots, p-1$ . Другим способом доказательства теоремы Ферма является получение того же самого из формулы  $\binom{p}{j} = p! / j! (p-j)!$ . (Поскольку  $p$  простое, множитель  $p$  в числителе не сокращается с множителями знаменателя.) Это дает  $(x + y)^p \equiv x^p + y^p \pmod{p}$  для любых целых  $x$  и  $y$ . Следовательно,  $(x + y + z)^p \equiv (x + y)^p + z^p \equiv x^p + y^p + z^p \pmod{p}$  и, в более общей форме,  $(\sum x_i)^p \equiv \sum x_i^p \pmod{p}$  для любой конечной суммы  $\sum x_i$  целых чисел. В частности, если  $x = 1 + 1 + \dots + 1$ , то  $x^p = (1 + 1 + \dots + 1)^p \equiv 1^p + 1^p + \dots + 1^p = x \pmod{p}$ , что и является теоремой Ферма.



жительное целое число, для которого  $p^f \equiv 1 \pmod{\lambda}$ . Это  $f$  называется *показателем числа  $p$  по модулю  $\lambda$* . Тогда  $f \mid (\lambda - 1)$ . Покажем, что  $g(\alpha) = g(\alpha^p)$  тогда и только тогда, когда  $g(\alpha)$  является круговым целым, образованным периодами длины  $f$ , где  $f$  — показатель числа  $p$  по модулю  $\lambda$ . Предположим сначала, что  $g(\alpha)$  образовано периодами длины  $f$ . Тогда, как мы видели в предыдущем параграфе,  $\sigma^e g(\alpha) = g(\alpha)$ , где  $e = (\lambda - 1)/f$ , а  $\sigma$  — сопряжение  $\alpha \mapsto \alpha^\gamma$  при некотором примитивном корне  $\gamma$  по модулю  $\lambda$ . Так как каждое сопряжение является степенью сопряжения  $\sigma$ , то  $\tau = \sigma^k$  при некотором  $k$ . Так как  $\tau^f = \sigma^{kf}$  — тождественное сопряжение, то  $kf$  делится на  $\lambda - 1 = ef$ . Таким образом,  $e$  делит  $k$ ,  $\tau$  есть степень сопряжения  $\sigma^e$  и  $\tau g(\alpha) = g(\alpha)$ , что и нужно было показать. Обратно, допустим, что  $\tau g(\alpha) = g(\alpha)$ . Как уже было показано,  $e \mid k$ . По определению,  $e \mid (\lambda - 1)$ . Таким образом,  $e$  — общий делитель чисел  $k$  и  $\lambda - 1$ . Он является наибольшим общим делителем, поскольку если  $d$  делит оба эти числа, например  $k = qd$  и  $\lambda - 1 = df'$ , то сопряжение  $\tau^{f'} = \sigma^{kf'} = \sigma^{qdf'} = (\sigma^{\lambda-1})^q$  является тождественным, откуда следует, что  $f' \geq f$  и  $d \leq e$ . Значит,  $e = ak + b(\lambda - 1)$  для некоторых целых  $a$  и  $b$ ,  $\sigma^e = \sigma^{ak} \sigma^{b(\lambda-1)} = \tau^a$ ,  $\sigma^e g(\alpha) = \tau^a g(\alpha) = g(\alpha)$ , что и требовалось доказать.

Это, в частности, показывает, что круговые целые, образованные периодами длины  $f$ , удовлетворяют сформулированному выше необходимому условию:  $g(\alpha) \equiv g(\alpha^p) \pmod{h(\alpha)}$  для  $g(\alpha)$ , сравнимого с целым числом по модулю  $h(\alpha)$ . Куммер доказал, что они и на самом деле сравнимы с целыми числами по модулю  $h(\alpha)$ .

**Теорема.** Пусть  $h(\alpha)$  — простое круговое целое,  $p$  — простое целое число, которое делится на  $h(\alpha)$ ,  $f$  — показатель числа  $p$  по модулю  $\lambda$  и  $\eta_i$  — период длины  $f$ . Тогда существует такое целое число  $u_i$ , что  $\eta_i \equiv u_i \pmod{h(\alpha)}$ . Следовательно, каждое круговое целое, образованное периодами длины  $f$ , сравнимо с некоторым целым числом по модулю  $h(\alpha)$ .

**Доказательство.** Эта теорема также опирается на некоторое обобщение теоремы Ферма, а именно, на сравнение

$$X^p - X \equiv (X - 1)(X - 2) \dots (X - p) \pmod{p},$$

которое означает, что все коэффициенты полинома  $X^p - X - (X - 1)(X - 2) \dots (X - p)$  делятся на  $p$ . Так как степень этого полинома меньше  $p$ , то для доказательства этого сравнения, как и раньше, достаточно доказать, что все его значения при целых  $X$  делятся на  $p$ . Но все значения полинома  $X^p - X$  при целых  $X$  сравнимы с нулем по модулю  $p$  (согласно теореме Ферма), тогда как все значения полинома  $(X - 1)(X - 2) \dots (X - p)$  являются произведениями  $p$  последовательных целых чисел, одно

из которых должно делиться на  $p$ , поэтому и они сравнимы с нулем по модулю  $p$ .

Отсюда следует, что для любого кругового целого  $g(\alpha)$  имеет место сравнение  $g(\alpha)^p - g(\alpha) \equiv [g(\alpha) - 1][g(\alpha) - 2] \dots [g(\alpha) - p] \pmod{p}$ . Значит,  $g(\alpha^p) - g(\alpha) \equiv [g(\alpha) - 1] \times \times [g(\alpha) - 2] \dots [g(\alpha) - p] \pmod{p}$ , и тем более это сравнение имеет место по модулю  $h(\alpha)$ . Если  $g(\alpha)$  образовано периодами длины  $f$ , то  $g(\alpha^p) - g(\alpha) = 0$ , а это дает  $[g(\alpha) - 1][g(\alpha) - 2] \dots [g(\alpha) - p] \equiv 0 \pmod{h(\alpha)}$ . Так как  $h(\alpha)$  простое, один из сомножителей  $g(\alpha) - 1, g(\alpha) - 2, \dots, g(\alpha) - p$  должен делиться на  $h(\alpha)$ , т. е.  $g(\alpha)$  сравнимо с некоторым целым числом по модулю  $h(\alpha)$ , что и требовалось доказать. В частности, каждый период  $\eta_i$  сам сравним с целым числом, которое мы, следуя Куммеру, обозначим через  $u_i$ .

Таблица умножения для периодов  $\eta_i$  индуцирует соотношения между целыми числами  $u_i$  по модулю  $p$ , точно так же как в § 4.3 из соотношения  $1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1} = 0$  следовало для целого числа  $k$  соотношение  $1 + k + k^2 + \dots + k^{\lambda-1} \equiv \equiv 0 \pmod{p}$ . В следующем параграфе рассматриваются различные конкретные примеры. В каждом из них можно найти все решения  $u_1, u_2, \dots, u_e$  этих сравнений по модулю  $p$  (где  $e = (\lambda - 1)/f$  является числом различных периодов длины  $f$ ) и, следовательно, определить, какие круговые целые, образованные периодами длины  $f$ , делятся на гипотетический простой делитель  $h(\alpha)$  числа  $p$ , даже не зная самого  $h(\alpha)$ . В большинстве случаев будет возможно даже найти круговое целое  $g(\alpha)$ , образованное периодами длины  $f$ , которое делится на гипотетический  $h(\alpha)$  и удовлетворяет условию  $Ng(\alpha) = p^f$ . Затем отсюда будет следовать, что если  $p$  имеет простой делитель  $h(\alpha)$ , то  $h(\alpha)$  делит одно из сопряженных элемента  $g(\alpha)$ ; так как  $Nh(\alpha)$  делит  $Np = p^{\lambda-1}$  и  $Nh(\alpha) \equiv h(1)^{\lambda-1} \equiv \equiv 0$  или  $1 \pmod{(\alpha - 1)}$ , то  $Nh(\alpha) \equiv 0$  или  $1 \pmod{\lambda}$ , т. е.  $Nh(\alpha)$  должно быть степенью числа  $p^f$ . Наконец, из  $h(\alpha) \mid g(\alpha)$  вытекает  $Nh(\alpha) = Ng(\alpha) = p^f$ . Короче, если  $p$  имеет простой делитель  $h(\alpha)$ , то  $h(\alpha)$  есть единица, умноженная на круговое целое, сопряженное элементу  $g(\alpha)$ .

В терминологии § 4.3 это рассуждение завершает анализ — оно дает очень сильные необходимые условия на простые круговые целые  $h(\alpha)$ , настолько сильные, что в примерах следующего параграфа мы сумеем найти все круговые целые  $h(\alpha)$ , которые могли бы быть простыми делителями данного  $p$ . Аналогом синтеза § 4.4 было бы доказательство того, что эти возможные простые делители на самом деле простые, т. е. если  $g(\alpha)$  — круговое целое, образованное периодами длины  $f$ , для которого  $Ng(\alpha) = p^f$ , где  $p$  — простое число, показатель которого по модулю  $\lambda$  есть  $f$ , то  $g(\alpha)$  просто. Хотя эта теорема верна, ее доказательство значи-

тельно труднее доказательства частного случая  $f = 1$  в § 4.3 и здесь, по-видимому, еще не стоит его приводить. Мы отложим его до § 4.11. Это означает, что в следующих двух параграфах еще не будет доказана простота круговых целых  $h(\alpha)$ , удовлетворяющих условию  $Nh(\alpha) = p^f$ , хотя в действительности они являются простыми. Удобно, однако, называть их простыми, понимая, что в свое время это будет доказано.

## Упражнения

1. При помощи треугольника Паскаля найдите все биномиальные коэффициенты  $\binom{n}{j}$  для  $n \leq 13$ . Проверьте непосредственно, что когда  $n$  простое и  $0 < j < n$ , коэффициенты делятся на  $n$  во всех случаях  $n \leq 13$ .

2. Подсчитайте полином  $X(X-1)(X-2)\dots(X-p+1)$  для  $p = 3, 5, 7, 11$ . (Каждое вычисление есть часть следующего.) Проверьте в каждом случае, что результат сравним с  $X^p - X$  по модулю  $p$ .

3. Проверьте формулу  $\eta^p \equiv \eta \pmod{p}$  в случае  $\lambda = 7, p = 2$ , найдя в явном виде  $f$ , все периоды длины  $f$  и  $p$ -ю степень каждого из них. Прделайте это же для  $\lambda = 13, p = 3$ .

4. Покажите, что для любого простого  $\lambda$  и любого целого  $k$  все простые делители суммы  $k^{\lambda-1} + k^{\lambda-2} + \dots + 1$  сравнимы либо с 0, либо с 1 по модулю  $\lambda$ .

5. Покажите, что в случае  $\lambda = 5, p = 19$  если  $p$  имеет простой делитель, то целые числа  $u_i$ , гарантированные теоремой в тексте, удовлетворяют условию  $u^2 + u - 1 \equiv 0 \pmod{19}$ . Найдите решения  $u$  этого сравнения. Затем покажите, что  $\eta_0 - u$  делит 19, и найдите разложение числа 19. Покажите, что сомножители в этом разложении неразложимы. (На самом деле, как будет позже доказано в этой главе, они простые.)

6. Используя процедуру предыдущего упражнения, найдите разложение числа 3 на неразложимые сомножители в случае  $\lambda = 13$ . (Опять же эти сомножители в действительности простые.)

7. Докажите, что если  $f$  — показатель числа  $p$  по модулю  $\lambda$  и  $g(\alpha)$  — круговое целое, для которого  $Ng(\alpha) = p^f$ , то  $g(\alpha)$  неразложимо.

## 4.7. Вычисления при $p \not\equiv 1 \pmod{\lambda}$

Показатель  $f$  простого числа  $p$  по модулю  $\lambda$  делит  $\lambda - 1$ , поэтому в случае  $\lambda = 5$  единственными возможными значениями для  $f$  являются 1, 2, 4. Случай  $f = 1$  был рассмотрен в § 4.4. В случае  $f = 4$  предположение  $h(\alpha) \mid p$ ,  $Nh(\alpha) \mid p^4$  вместе с тем фактом, что  $Nh(\alpha) \equiv [h(1)]^4 \pmod{(\alpha-1)}$ ,  $Nh(\alpha) \equiv 0$  или  $1 \pmod{\lambda}$ , дает  $p^f \mid Nh(\alpha) \mid p^4$ ,  $Nh(\alpha) = Nr$ , откуда следует, что  $h(\alpha)$  есть единица, умноженная на  $p$ . Короче, *единственными возможными простыми делителями простых чисел  $p = 2, 3, 7, 13, \dots$  показателя 4 по модулю 5 являются единицы, умноженные на само  $p$* . Остается только найти простые делители числа  $p$  в случае  $f = 2$ . Такими простыми являются 19, 29, 59, 79, 89,  $\dots$ , сравнимые с 4 по модулю 5 (1 имеет показатель 1; 4 — показатель 2; 2 и 3 — показатель 4 по модулю 5).

В случае  $\lambda = 5, f = 2$  интересующими нас периодами являются  $\eta_0 := \alpha + \alpha^4$ ,  $\eta_1 = \alpha^2 + \alpha^3$ . (Нумерация периодов не зависит от того, какое  $\gamma$  мы выберем:  $\gamma = 2$  или  $\gamma = 3$ .) В таком случае, как этот, когда  $f = (\lambda - 1)/2$ ,  $e = 2$ , лучше обозначить периоды через  $\theta_0, \theta_1$ , а не  $\eta_0, \eta_1$ . Поскольку  $1 + \theta_0 + \theta_1 = 0$ , любое круговое целое  $a + b\theta_0 + c\theta_1$ , образованное перио-

дами длины 2, может быть записано в виде  $A + B\theta_0$  ( $A = a - c$ ,  $B = b - c$ ), а его норма — в виде  $(A + B\theta_0)(A + B\theta_1)(A + B\theta_0)(A + B\theta_1) = [A^2 + AB(\theta_0 + \theta_1) + B^2\theta_0\theta_1]^2 = [A^2 - AB - B^2]^2$ , ибо, как показывает простое вычисление,  $\theta_0\theta_1 = -1$ . Как указывалось в конце предыдущего параграфа, задача состоит в том, чтобы для данного  $p$  с показателем 2 по модулю 5 сначала найти целые числа  $u_0, u_1$ , для которых возможны сравнения  $\theta_0 \equiv u_0$ ,  $\theta_1 \equiv u_1$  по модулю  $h(\alpha)$ , а затем найти круговое целое  $g(\alpha) = a + b\theta_0 + c\theta_1$ , удовлетворяющее условиям  $a + bu_0 + cu_1 \equiv 0 \pmod{p}$  и  $Ng(\alpha) = p^2$ . В частности, далее задача заключается в нахождении для каждого  $p = 19, 29, 59, \dots$  такого кругового целого  $A + B\theta_0$ , для которого  $A^2 - AB - B^2 = \pm p$ .

Как и в случае  $f = 1$ , некоторый успех достигается путем проб и ошибок. В табл. 4.7.1 показаны значения величины  $A^2 - AB - B^2$  для некоторых

Таблица 4.7.1

$A$	$B$	$A^2 - AB - B^2$
2	1	1
2	-1	5
3	1	5
3	-1	11
3	2	-1
3	-2	11
4	1	11
4	-1	19
4	3	-5
4	-3	19
5	1	19
5	-1	29

малых  $A$  и  $B$ . (Можно считать, что  $A$  и  $B$  взаимно просты,  $A$  — большее из двух этих чисел по абсолютной величине и  $A > 0$ .) Так как  $(4 - \theta_0)(4 - \theta_1) = 19$ , рассуждения предыдущего параграфа показывают, что единственными возможными простыми делителями числа 19 являются единицы, умноженные на сопряженные элемента  $4 - \theta_0$ . Очевидно, что по модулю  $4 - \theta_0$  имеют место сравнения  $\theta_0 \equiv 4$  и  $\theta_1 = -1 - \theta_0 \equiv -1 - 4 = -5$ . Следовательно,  $a + b\theta_0 + c\theta_1 \equiv a + 4b - 5c$  и  $a + b\theta_0 + c\theta_1$  делится на  $4 - \theta_0$  тогда и только тогда, когда  $a + 4b - 5c \equiv 0 \pmod{19}$ . Аналогично, единственными возможными делителями числа 29 являются единицы, умноженные на сопряженные элемента  $5 - \theta_0$ , и  $5 - \theta_0$  делит  $a + b\theta_0 + c\theta_1$  тогда и только тогда, когда  $a + 5b - 6c \equiv 0 \pmod{29}$ . Это дает разложение на про-

стые <sup>1)</sup> сомножители  $19 = (4 - \theta_0)(4 - \theta_1)$  и  $29 = (5 - \theta_0)(5 - \theta_1)$  чисел 19 и 29, а также признак делимости на эти простые сомножители.

Чтобы достичь следующего простого числа 59 с показателем 2 по модулю 5, таблицу 4.7.1 нужно было бы продолжить значительно дальше. Поэтому стоит испытать метод, предложенный в предыдущем параграфе. А именно, если бы простой делитель был известен, то имелись бы целые числа  $u_0$  и  $u_1$ , с которыми периоды  $\theta_0$  и  $\theta_1$  были бы сравнимы по модулю этого делителя. Так как  $1 + \theta_0 + \theta_1 = 0$  и  $\theta_0\theta_1 = -1$ , то эти целые числа удовлетворяли бы сравнениям  $1 + u_0 + u_1 \equiv 0$ ,  $u_0u_1 \equiv -1$  по модулю делителя числа 59, а следовательно, по модулю 59. Эти два сравнения с двумя неизвестными можно свести к одному с одним неизвестным:  $u_0(-1 - u_0) \equiv -1$ ,  $u_0^2 + u_0 - 1 \equiv 0 \pmod{59}$ . Решение этого сравнения можно найти следующим образом. Имеем  $u_0(u_0 + 1) = 1 + 59n$  для некоторого  $n$ . Так как  $u_0(u_0 + 1)$  четно,  $n$  должно быть нечетным. Так как  $u_0(u_0 + 1)$  неотрицательно ( $u_0$  целое),  $n$  должно быть положительным. Испробовав  $n = 1, 3, 5, \dots$ , найдем  $60 = 2^2 \cdot 3 \cdot 5$ ,  $178 = 2 \cdot 89$ ,  $296 = 2^3 \cdot 37$ ,  $414 = 2 \cdot 3^2 \cdot 23$ ,  $532 = 2^2 \cdot 7 \cdot 19$ ,  $650 = 2 \cdot 5^2 \cdot 13$ ,  $\dots$ . Первое из этих чисел, которое может быть записано в виде  $u_0(u_0 + 1)$ , есть  $650 = 25 \cdot 26$ . Это дает решение  $u_0 = 25$ ,  $u_1 = -26$ . Сравнение  $u^2 + u - 1 \equiv 0 \pmod{59}$  имеет не более двух решений; значит, оно имеет лишь решения 25, -26. Так как из  $u_0 \equiv 25$  вытекает  $u_1 \equiv -26$ , а из  $u_0 \equiv -26$  вытекает  $u_1 \equiv 25$ , то эти числа составляют единственно возможную пару значений  $u_0, u_1$  по модулю 59. Круговое целое вида  $a + b\theta_0 + c\theta_1$

<sup>1)</sup> Как было отмечено в конце предыдущего параграфа, доказательство того, что эти сомножители действительно простые, будет дано в § 4.11.

тогда и только тогда делится на гипотетический делитель числа 59, по модулю которого  $u_0 \equiv 25$ , когда  $a + 25b - 26c \equiv 0 \pmod{59}$ . Например, на него делится  $25 - \theta_0$ . Далее,  $N(25 - \theta_0) = (625 + 25 - 1)^2 = 11^2 \cdot 59^2$ . Следовательно, искомый делитель числа 59 можно найти делением числа  $25 - \theta_0$  на два подходящих делителя числа 11. По модулю простого делителя  $\alpha + 2$  числа 11 (см. табл. 4.4.1) имеем:  $\theta_0 = \alpha + \alpha^4 \equiv -2 + (-2)^4 \equiv 3$  и  $\theta_1 = \alpha^2 + \alpha^3 \equiv -4$ . Следовательно, число  $25 - \theta_0$  делится на  $\alpha + 2$ , поскольку  $25 - 3 \equiv 0 \pmod{11}$ . Оно также делится на  $\alpha^4 + 2$ , поскольку сопряжение  $\alpha \mapsto \alpha^4$  оставляет  $\theta_0$  и  $\theta_1$  без изменения. Значит, искомый делитель должен быть следующим:

$$\begin{aligned} \frac{25 - \theta_0}{(\alpha + 2)(\alpha^4 + 2)} &= \frac{25 - \theta_0}{1 + 2\theta_0 + 4} = \frac{(25 - \theta_0)(5 + 2\theta_1)}{(5 + 2\theta_0)(5 + 2\theta_1)} = \\ &= \frac{125 - 5\theta_0 + 50\theta_1 + 2}{25 - 10 - 4} = \frac{132 + 55\theta_1}{11} = 12 + 5\theta_1. \end{aligned}$$

Таким образом, равенство  $59 = (12 + 5\theta_1)(12 + 5\theta_0)$  и есть искомое разложение числа 59 на простые сомножители.

Следующее простое число, которое нужно разложить, есть 79. Способ, примененный в случае числа 59, позволяет установить, что  $11 \cdot 79 + 1 = 870 = 29 \cdot 30$ . Признаком делимости, следовательно, является сравнение  $a + 29b - 30c \equiv 0 \pmod{79}$ . Решение этого сравнения в относительно небольших целых числах есть  $b = 3$ ,  $a = -8$ ,  $c = 0$ . Так как  $(-8 + 3\theta_0) \times (-8 + 3\theta_1) = 64 + 24 - 9 = 79$ , то это дает нам разложение числа 79. Следующее простое число 89 разлагается очень легко:  $89 + 1 = 9 \cdot 10$ ; признак делимости есть  $a + 9b - 10c \equiv 0 \pmod{89}$ , находится число  $\theta_0 - 9$ ,

Таблица 4.7.2.  $\lambda = 5$ ,  $f = 2$

простое	норма	$\theta_0 \equiv$	$\theta_1 \equiv$
$\theta_0 - 4$	$19^2$	4	-5
$\theta_0 - 5$	$29^2$	5	-6
$5\theta_0 + 12$	$59^2$	-26	25
$3\theta_0 - 8$	$79^2$	29	-30
$\theta_0 - 9$	$89^2$	9	-10

и тогда  $(\theta_0 - 9)(\theta_1 - 9) = 89$ . Это завершает разложение простых чисел, меньших 100. Результаты показаны в табл. 4.7.2 (и в табл. 4.4.1).

Когда  $\lambda = 7$ , показателями  $f$  числа  $p$  по модулю  $\lambda$  должны быть 1, 2, 3 или 6, поскольку  $f \mid (\lambda - 1)$  и  $\lambda - 1 = 6$ . Случай  $f = 1$  был разобран в § 4.4, а случай  $f = 6$  неинтересен, поскольку в этом случае  $p$  не имеет нетривиальных разложений. Случай  $f = 3$  имеет место, когда  $p \equiv 2$  или 4 по модулю 7. Такими являются простые  $p = 2, 11, 23, 37, 53, \dots$ . Случай  $f = 2$  имеет место, когда  $p \equiv -1 \pmod{7}$ ,  $p = 13, 41, 83, \dots$ . Первым рассмотрим случай  $f = 3$ .

Периодами длины 3 являются  $\theta_0 = \alpha + \alpha^2 + \alpha^4$ ,  $\theta_1 = \alpha^3 + \alpha^5 + \alpha^6$  (не существенно, использовано ли  $\gamma = 3$  или  $\gamma = 5$ ). Имеем  $1 + \theta_0 + \theta_1 = 0$  и  $\theta_0\theta_1 = \alpha^4 + \alpha^6 + 1 + \alpha^5 + 1 + \alpha + 1 + \alpha^2 + \alpha^3 = 2$ . Следовательно,

каждое круговое целое, образованное периодами длины 3, имеет вид  $A + B\theta_0$ , а его норма есть  $(A + B\theta_0)^3 (A + B\theta_1)^3 = (A^2 - AB + 2B^2)^3$ . В этом случае все небольшие простые числа очень легко разложить путем проб и ошибок. Дело сводится к отысканию пары таких целых чисел  $A, B$ , что

Таблица 4.7.3

$A$	$B$	$A^2 - AB + 2B^2$
1	2	7
1	4	29
1	6	67
3	2	11
3	4	29
5	2	23
5	4	37
5	6	67
7	2	43
7	4	53
7	6	79
9	2	71
9	4	77

$A^2 - AB + 2B^2 = p$ , где  $p = 2, 11, 23, 37, \dots$ . Для  $p = 2$  решение получается непосредственно, и соответствующее разложение числа 2 имеет вид  $2 = \theta_0\theta_1$ . Для нечетных простых чисел ясно, что  $A$  должно быть нечетным, а  $B$  — четным. Так как эти числа должны быть к тому же взаимно простыми, то имеет смысл делать только те пробы, которые показаны в табл. 4.7.3 (для  $p < 100$ ). Искомые разложения можно тогда взять из этой таблицы:  $67 = (1 + 6\theta_0)(1 + 6\theta_1)$ ,  $11 = (3 + 2\theta_0) \times (3 + 2\theta_1)$  и т. д. Чтобы найти целые числа, с которыми  $\theta_0$  и  $\theta_1$  сравнимы по модулю этих простых круговых целых, нужно только решить простое линейное сравнение. Например, если  $\theta_0 \equiv k \pmod{1 + 6\theta_0}$ , то  $1 + 6k \equiv 0 \pmod{1 + 6\theta_0}$ ,  $6k \equiv -1 \pmod{67}$ ,  $66k \equiv -11 \pmod{67}$ ,  $k \equiv 11 \pmod{67}$ . Эти разложения приведены в табл. 4.7.4.

Теперь рассмотрим случай  $\lambda = 7, f = 2$ . Периодами длины 2 являются  $\eta_0 = \alpha + \alpha^6, \eta_1 = \alpha^3 + \alpha^4, \eta_2 = \alpha^2 + \alpha^5$ , где использован примитивный корень  $\gamma = 3$ . (Если использовать  $\gamma = 5$ , то периоды останутся такими же,

Таблица 4.7.4.  $\lambda = 7, f = 3$

простое	норма	$\theta_0 \equiv$	$\theta_1 \equiv$
$\theta_0$	$2^3$	0	1
$2\theta_0 + 3$	$11^3$	4	- 5
$2\theta_0 + 5$	$23^3$	9	- 10
$4\theta_0 + 5$	$37^3$	8	- 9
$4\theta_0 + 7$	$53^3$	- 15	14
$6\theta_0 + 1$	$67^3$	11	- 12
$6\theta_0 + 7$	$79^3$	12	- 13

но изменятся их номера.) Как легко проверить прямым вычислением, они удовлетворяют уравнениям  $1 + \eta_0 + \eta_1 + \eta_2 = 0, \eta_0^2 = 2 + \eta_2$  и  $\eta_0\eta_1 = \eta_1 + \eta_2$ . Другие соотношения между ними можно найти из этих посредством сопряжений, которые осуществляются циклической перестановкой периодов  $\eta_i$ :  $\eta_1^2 = 2 + \eta_0, \eta_2^2 = 2 + \eta_1, \eta_1\eta_2 = \eta_2 + \eta_0, \eta_2\eta_0 = \eta_0 + \eta_1$ . Первое простое число, которое надо разложить, есть 13. Пусть  $u_0, u_1, u_2$  — те целые числа, с которыми сравнимы  $\eta_0, \eta_1, \eta_2$  по модулю простого делителя



числа 13 (если таковой имеется); тогда имеют место сравнения

$$1 + u_0 + u_1 + u_2 \equiv 0 \pmod{13}$$

$$u_0^2 \equiv 2 + u_2 \pmod{13}$$

$$u_0 u_1 \equiv u_1 + u_2 \pmod{13}$$

и сравнения, получаемые из этих циклическими перестановками индексов. Таким образом,

$$\begin{aligned} u_0^3 &\equiv 2u_0 + u_0 u_2 \equiv 2u_0 + u_0 + u_1 \equiv \\ &\equiv -1 + 2u_0 - u_2 \equiv \\ &\equiv -1 + 2u_0 + 2 - u_0^2 \end{aligned}$$

$$u_0^3 + u_0^2 - 2u_0 - 1 \equiv 0 \pmod{13}$$

Этому сравнению не удовлетворяют  $u_0 = 0, \pm 1, \pm 2$  и  $3$ , но удовлетворяет  $u_0 = -3$ . Далее, этим определяются значения других неизвестных:  $u_2 \equiv u_0^2 - 2 \equiv 7 \equiv -6 \pmod{13}$  и  $u_1 \equiv -1 - u_0 - u_2 \equiv -1 + 3 + 6 = 8 \equiv -5 \pmod{13}$ . Заметим, что, как и ожидалось,  $u_0 \equiv -5$  и  $u_0 \equiv -6$  также являются решениями сравнения для  $u_0$ , и если использовать любое из них, то этим определяются значения двух других неизвестных. Значит, поскольку сравнение степени 3 по простому модулю имеет не более 3 решений, *единственными возможными* решениями  $(u_0, u_1, u_2)$ , удовлетворяющими первоначальному сравнению, являются  $(-3, -5, -6)$ ,  $(-5, -6, -3)$  и  $(-6, -3, -5)$ . Следовательно,  $a + b\eta_0 + c\eta_1 + d\eta_2$  делится на простой делитель числа 13, только если это круговое целое или одно из его сопряженных удовлетворяет условию  $a - 3b - 5c - 6d \equiv 0 \pmod{13}$ . Например,  $1 - \eta_1 + \eta_2$  или одно из его сопряженных могли бы делиться на простой делитель числа 13. Произведение трех различных сопряженных равно

$$\begin{aligned} (1 - \eta_1 + \eta_2)(1 - \eta_2 + \eta_0)(1 - \eta_0 + \eta_1) &= \\ &= (1 - \eta_1 + \eta_2)(1 - \eta_0 + \eta_1 - \eta_2 + \eta_0 + \eta_1 - \eta_2 - \eta_0 + \eta_0 - 2 - \eta_2 + \eta_1 + \eta_2) = \\ &= (1 - \eta_1 + \eta_2)(-1 + 3\eta_1 - 2\eta_2) = \\ &= -1 + 3\eta_1 - 2\eta_2 + \eta_1 - 3(2 + \eta_0) + 2(\eta_2 + \eta_0) - \eta_2 + 3(\eta_2 + \eta_0) - 2(2 + \eta_1) = \\ &= -11 + 2\eta_0 + 2\eta_1 + 2\eta_2 = -13. \end{aligned}$$

Это и дает разложение:  $13 = (\eta_1 - \eta_2 - 1)(\eta_2 - \eta_0 - 1)(\eta_0 - \eta_1 - 1)$ .

Следующим простым числом с показателем 2 по модулю 7 является 41. Как и для 13,  $u_0$  должно удовлетворять сравнению  $u_0^3 + u_0^2 - 2u_0 - 1 \equiv 0 \pmod{41}$ . Значения  $u_0 \equiv 0, \pm 1, \pm 2, \pm 3, 4$  сразу же отвергаются, но  $u_0 \equiv -4$  удовлетворяет сравнению. Тогда  $u_2 \equiv u_0^2 - 2 \equiv 14$  и  $u_1 \equiv -1 - u_0 - u_2 \equiv -11$ . Снова  $-4, -11, 14$  оказываются полным набором решений сравнения для  $u_0$ , которые и определяют значения неизвестных  $u_1$  и  $u_2$ . Значит, если  $a + b\eta_0 + c\eta_1 + d\eta_2$  делится на простой делитель числа 41, то оно или одно из его сопряженных должно удовлетворять условию  $a - 4b - 11c + 14d \equiv 0 \pmod{41}$ . Например, мы можем испытать  $4 + \eta_0$ . Этот

выбор успешен, поскольку

$$\begin{aligned}(4 + \eta_0)(4 + \eta_1)(4 + \eta_2) &= (4 + \eta_0)(16 + 4\eta_1 + 4\eta_2 + \eta_2 + \eta_0) = \\ &= (4 + \eta_0)(12 - 3\eta_0 + \eta_2) = 48 - 12\eta_0 + 4\eta_2 + 12\eta_0 - 3(2 + \eta_2) + (\eta_0 + \eta_1) = \\ &= 42 + \eta_0 + \eta_1 + \eta_2 = 41\end{aligned}$$

что и дает разложение числа 41.

Из простых чисел, меньших 100 и имеющих показатель 2 по модулю 7, остаются только 83 и 97. Решение сравнения  $u_0^3 + u_0^2 - 2u_0 - 1 \equiv 0 \pmod{83}$  просто путем проб и ошибок требует некоторого терпения. В конце концов мы найдем решение  $u_0 \equiv 10$ , откуда получаем другие два решения  $u_2 \equiv 100 - 2 \equiv 15$ ,  $u_1 \equiv -1 - 10 - 15 = -26$ . Это приводит к рассмотрению таких  $a + b\eta_0 + c\eta_1 + d\eta_2$ , для которых  $a + 10b - 26c + 15d \equiv 0 \pmod{83}$ , например  $5 + \eta_0 - \eta_2$ . Короткое вычисление показывает, что  $(5 + \eta_0 - \eta_2)(5 + \eta_1 - \eta_0)(5 + \eta_2 - \eta_1) = 83$  и  $(4\eta_0 - 3)(4\eta_1 - 3) \cdot (4\eta_2 - 3) = 97$ . Этим завершается нахождение разложений простых чисел  $p < 100$  при  $\lambda = 7$ . Результаты даются в таблицах 4.7.5, 4.7.4 и 4.4.2.

Таблица 4.7.5.  $\lambda = 7, f = 2$

простое	норма	$\eta_0 \equiv$	$\eta_1 \equiv$	$\eta_2 \equiv$
$\eta_1 - \eta_2 - 1$	$13^2$	$-3$	$-5$	$-6$
$\eta_0 + 4$	$41^2$	$-4$	$-11$	$14$
$\eta_0 - \eta_2 + 5$	$83^2$	$10$	$-26$	$15$
$4\eta_0 - 3$	$97^2$	$25$	$30$	$41$

В качестве еще одного примера рассмотрим случай  $\lambda = 13, p = 29$ . В этом случае  $p \equiv 3, p^2 \equiv 9, p^3 \equiv 1 \pmod{\lambda}$ . Значит,  $f = 3$ . Как было найдено в § 4.4, периодами длины 3 являются  $\eta_0 = \alpha + \alpha^3 + \alpha^9, \eta_1 = \alpha^2 + \alpha^5 + \alpha^6, \eta_2 = \alpha^4 + \alpha^{10} + \alpha^{12}, \eta_3 = \alpha^8 + \alpha^7 + \alpha^{11}$ , где в качестве примитивного корня по модулю 13 использовано либо  $\gamma = 2$ , либо  $\gamma = 6$ . (Если  $\gamma = -2$  или  $-6$ , то сами периоды не изменятся, а изменится лишь их нумерация.) Кроме того, они удовлетворяют соотношениям

$$1 + \eta_0 + \eta_1 + \eta_2 + \eta_3 = 0$$

$$\eta_0^2 = \eta_1 + 2\eta_2$$

$$\eta_0\eta_1 = \eta_0 + \eta_1 + \eta_3$$

$$\eta_0\eta_2 = 3 + \eta_1 + \eta_3$$

$$\eta_0\eta_3 = (\text{из } \eta_0\eta_1)$$

и соотношениям, получаемым из этих циклическими перестановками  $\eta_0 \mapsto \eta_1 \mapsto \eta_2 \mapsto \eta_3 \mapsto \eta_0$ . Если  $u_0, u_1, u_2, u_3$  — целые числа, сравнимые с  $\eta_0, \eta_1, \eta_2, \eta_3$  по модулю простого делителя числа 29 (при условии, что 29 имеет

простой делитель), то выполняются сравнения

$$1 + u_0 + u_1 + u_2 + u_3 \equiv 0 \pmod{29}$$

$$u_0^2 \equiv u_1 + 2u_2 \pmod{29}$$

$$u_0u_1 \equiv u_0 + u_1 + u_3 \pmod{29}$$

$$u_0u_2 \equiv 3 + u_1 + u_3$$

и сравнения, получаемые из них циклической перестановкой неизвестных  $u_i$ . Далее,

$$u_0^3 \equiv u_0u_1 + 2u_0u_2 \equiv u_0 + u_1 + u_3 + 2(3 + u_1 + u_3) \equiv$$

$$\equiv 6 + u_0 + 3u_1 + 3u_3 \equiv 3 - 2u_0 - 3u_2$$

$$u_0^4 \equiv 3u_0 - 2(u_1 + 2u_2) - 3(3 + u_1 + u_3) \equiv$$

$$\equiv -9 + 3u_0 - 5u_1 - 4u_2 - 3u_3 \equiv$$

$$\equiv -6 + 6u_0 - 2u_1 - u_2$$

$$u_0^4 + 2u_0^2 \equiv -6 + 6u_0 + 3u_2 \equiv -6 + 6u_0 + (3 - 2u_0 - u_0^3)$$

$$u_0^4 + u_0^3 + 2u_0^2 - 4u_0 + 3 \equiv 0 \pmod{29}$$

Сразу находим, что  $u_0 \equiv 0, \pm 1, \pm 2, 3$  не удовлетворяют этому уравнению, но  $u_0 \equiv -3$  удовлетворяет. Затем определяются  $3u_2 \equiv 3 - 2u_0 - u_0^3 \equiv \equiv 3 + 6 - 2 = 7$ ,  $30u_2 \equiv 70 \equiv 12$ ,  $u_2 \equiv 12$ ,  $u_1 \equiv u_0^2 - 2u_2 \equiv 9 - 24 \equiv 14$  и  $u_3 \equiv -1 - u_0 - u_1 - u_2 \equiv -1 + 3 - 12 - 14 \equiv 5$ . Единственными возможными решениями наших сравнений будут, следовательно, набор  $u_0 \equiv -3$ ,  $u_1 \equiv 14$ ,  $u_2 \equiv 12$ ,  $u_3 \equiv 5 \pmod{29}$ , а также наборы, получаемые из него циклическими перестановками, поскольку эти 4 целых числа являются единственными решениями сравнения  $u_0^4 + u_0^3 + 2u_0^2 - 4u_0 + 3 \equiv 0 \pmod{29}$ , а значения остальных трех компонент набора определяются выбором значения  $u_0$ . Следовательно, если число  $a + b\eta_0 + c\eta_1 + d\eta_2 + e\eta_3$  делится на простой делитель числа 29, то оно или одно из его сопряженных удовлетворяет условию  $a - 3b + 14c + 12d + 5e \equiv 0 \pmod{29}$ . Например, мы вправе испытать  $3 + \eta_0$ . Тогда  $(3 + \eta_0)(3 + \eta_2) = 9 + 3\eta_2 + 3\eta_0 + 3 + \eta_1 + \eta_3 = 12 + 3\theta_0 + \theta_1 = 11 + 2\theta_0$ , где  $\theta_0 = \eta_0 + \eta_2$ ,  $\theta_1 = \eta_1 + \eta_3$ . Произведение четырех сопряженных элемента  $3 + \eta_0$  есть, следовательно,  $(11 + 2\theta_0) \times (11 + 2\theta_1) = 121 - 22 + 4\theta_0\theta_1 = 121 - 34 = 87 = 3 \cdot 29$ , поскольку  $\theta_0\theta_1 = -3$ . Для нахождения делителя числа 29 необходимо разделить  $3 + \eta_0$  на подходящий делитель числа 3.

Большая часть работы, требующейся для разложения числа 3, была уже выполнена. Показатель числа 3 по модулю 13 равен 3, и разложение опирается на нахождение решений сравнения  $u_0^4 + u_0^3 + 2u_0^2 - 4u_0 + 3 \equiv \equiv 0 \pmod{3}$ . Решением является  $u_0 \equiv 0$ . Тогда все остальные неизвестные  $u_1 + u_3 \equiv 0$ ,  $u_2 \equiv -1 - u_0 - u_1 - u_3 \equiv -1$ ,  $u_1 \equiv u_0^2 - 2u_2 \equiv -1$ ,  $u_3 \equiv \equiv -u_1 \equiv 1$  определяются найденным значением  $u_0$ . Значит, делитель числа 3 мы ищем среди круговых целых  $a + b\eta_0 + c\eta_1 + d\eta_2 + e\eta_3$ , для которых  $a - c - d + e \equiv 0 \pmod{3}$ . Например, пусть  $b = 1$ ,  $a = c = d = e = 0$ . Тогда  $\eta_0\eta_2 = 3 + \theta_1$ ,  $\eta_0\eta_1\eta_2\eta_3 = (3 + \theta_0)(3 + \theta_1) = 9 - 3 - 3 = 3$ . Следовательно,  $\eta_0$  есть простой делитель числа 3, по модулю которого  $\eta_0 \equiv 0$ ,

$\eta_1 \equiv -1$ ,  $\eta_2 \equiv -1$ ,  $\eta_3 \equiv 1$ . Отсюда  $3 + \eta_0 \equiv 3 \equiv 0 \pmod{\eta_0}$ . Деление элемента  $3 + \eta_0 = \eta_0\eta_1\eta_2\eta_3 + \eta_0$  на  $\eta_0$  дает  $\eta_1\eta_2\eta_3 + 1 = \eta_2(3 + \eta_0 + \eta_2) + 1 = 3\eta_2 + 3 + \eta_1 + \eta_3 + \eta_3 + 2\eta_0 + 1 = 4 + 2\eta_0 + \eta_1 + 3\eta_2 + 2\eta_3 = 2 - \eta_1 + \eta_2$ , что и является делителем числа 29, по модулю которого  $\eta_0 \equiv -3$ ,  $\eta_1 \equiv 14$ ,  $\eta_2 \equiv 12$ ,  $\eta_3 \equiv 5$ .

Среди случаев с  $f > 1$ , так же как и в случаях с  $f = 1$ , имеются такие, когда этот метод не в состоянии осуществить разложение числа  $p$ . Примером служит случай  $\lambda = 31$ ,  $p = 2$ . Здесь  $f = 5$ , и если периоды длины 5 построены с помощью примитивного корня 3 по модулю 31, то для них имеют место равенства

$$\eta_0 = \alpha + \alpha^{-15} + \alpha^8 + \alpha^4 + \alpha^2$$

$$\eta_1 = \alpha^3 + \alpha^{-14} + \alpha^{-7} + \alpha^{12} + \alpha^6$$

$$\eta_2 = \alpha^9 + \alpha^{-11} + \alpha^{10} + \alpha^5 + \alpha^{-13}$$

$$\eta_3 = \alpha^{-4} + \alpha^{-2} + \alpha^{-1} + \alpha^{15} + \alpha^{-8}$$

$$\eta_4 = \alpha^{-12} + \alpha^{-6} + \alpha^{-3} + \alpha^{14} + \alpha^7$$

$$\eta_5 = \alpha^{-5} + \alpha^{13} + \alpha^{-9} + \alpha^{11} + \alpha^{-10}$$

$$\eta_0^2 = \eta_0 + 2\eta_1 + 2\eta_2$$

$$\eta_0\eta_1 = \eta_0 + \eta_2 + 2\eta_4 + \eta_5$$

$$\eta_0\eta_2 = \eta_1 + \eta_2 + \eta_4 + 2\eta_5$$

$$\eta_0\eta_3 = 5 + \eta_0 + \eta_1 + \eta_3 + \eta_4$$

$$\eta_0\eta_4 = (\text{из } \eta_0\eta_2)$$

$$\eta_0\eta_5 = (\text{из } \eta_0\eta_1)$$

Предположим, что  $u_0, u_1, u_2, u_3, u_4, u_5$  — целые числа, удовлетворяющие этим уравнениям относительно  $\eta_i$ , рассматриваемым как сравнения по модулю 2. Можно считать, что  $u_i = 0$  или 1. Рассматривая наборы  $u_i$  с точностью до циклических сдвигов, мы видим, что решение должно содержать либо два последовательных нуля, либо две последовательные единицы, поскольку 0, 1, 0, 1, 0, 1 и 1, 0, 1, 0, 1, 0 не удовлетворяют сравнению  $u_0u_3 \equiv 5 + u_0 + u_1 + u_3 + u_4 \pmod{2}$ . Если мы предположим, что  $u_0 = u_1 = 0$ , то сравнения  $0 \equiv 0 + u_2 + 2u_4 + u_5$ ,  $0 \equiv 0 + u_2 + u_4 + 2u_5$  и  $0 \equiv 5 + 0 + 0 + u_3 + u_4$  дают  $u_2 \equiv u_5 \equiv u_4 \equiv 1 + u_3$ . Из  $\eta_2\eta_4 = \eta_3 + \eta_4 + \eta_0 + 2\eta_1$  следует, что  $u_2u_4 \equiv 1 \pmod{2}$ , и этим определяется решение 0, 0, 1, 0, 1, 1. Аналогично, если  $u_0 \equiv 1$ ,  $u_1 \equiv 1$ , то этим определяется решение 1, 1, 0, 0, 1, 0. Таким образом, с точностью до циклических перестановок имеется только один возможный набор значений  $u_i$  по модулю 2. (Это не доказывает, однако, что этот набор значений  $u_i$  удовлетворяет всем соотношениям для  $\eta_i$ , рассматриваемым как сравнения по модулю 2. То что он действительно им удовлетворяет, следует из предложения ниже, в § 4.9.) Значит, если  $a + b\eta_0 + c\eta_1 + d\eta_2 + e\eta_3 + f\eta_4 + g\eta_5$  делится на делитель числа 2, то это круговое целое или одно из его сопряженных удовлетворяет условию  $a + d + f + g \equiv 0 \pmod{2}$ . Простейшим кандидатом является  $\eta_0$ . Однако  $\eta_0\eta_2\eta_4 = \eta_0(\eta_3 + \eta_4 + \eta_0 + 2\eta_1) = 5 + \eta_0 + \eta_1 + \eta_3 + \eta_4 + \eta_5 + \eta_0 + \eta_2 + 2\eta_3 + \eta_0 + 2\eta_1 + 2\eta_2 + 2(\eta_0 + \eta_2 + 2\eta_4 + \eta_5) = 5 + 5\eta_0 + 3\eta_1 + 5\eta_2 + 3\eta_3 + 5\eta_4 + 3\eta_5 = 2 + 2\theta_0$  (где  $\theta_0 = \eta_0 + \eta_2 + \eta_4$ ) и  $\eta_0\eta_1\eta_2\eta_3\eta_4\eta_5 = (2 + 2\theta_0)(2 + 2\theta_1) = 4 - 4 + 4\theta_0\theta_1 = 32$ , поскольку  $\theta_0\theta_1 = 8$ . Следовательно, нет не только этого предполагаемого делителя, но и никакого предполагаемого делителя такого типа, поскольку произведение его трех сопряженных имело бы вид  $X + Y\theta_0$ , а произведение всех шести было бы вида  $(X + Y\theta_0)(X + Y\theta_1) = X^2 - XY + 8Y^2 = (4X^2 - 4XY + 32Y^2)/4 = [(2X - Y)^2 + 31Y^2]/4$  при некоторых целых  $X$  и  $Y$ . Так как число 8 нельзя записать в виде  $a^2 + 31b^2$  при целых  $a$  и  $b$ , то это показывает, что произведение шести сопряженных не может равняться числу 2. В отличие от случая  $f = 1$ , однако, здесь невозможно столь доступным способом сделать заключение о том, что число 2 не имеет разложения на простые, но можно лишь утверждать, что оно не имеет такого разложения, в котором сомножители образованы периодами длины 5.

## Упражнения

1. Таблица 4.7.5 показывает, что при  $\lambda = 7$  элемент  $\eta_2 - \eta_1 + 1$  делит  $\eta_0 + 3$ . Покажите, что частное есть единица, и найдите ее и ее обратный элемент в явном виде.

2. Выведите последнюю строку табл. 4.7.5, т. е. разложите число 97 при  $\lambda = 7$ .

3. В случае  $\lambda = 13$  найдите одно простое число  $p$ , оставшееся после рассмотрения чисел 3 и 29, имеющее показатель 3 и меньшее 100. Запишите его как произведение четырех сомножителей, норма каждого из которых равна  $p^3$ . [Это вычисление довольно длинное, но ненамного длиннее вычисления в случае  $p = 29$ , проведенного в тексте. Сравнение для  $u$  решается значением  $u = 10$  и не решается никаким значением, меньшим по абсолютной величине.]

4. Продолжите табл. 4.7.2, чтобы захватить следующее простое число с показателем 2 по модулю 5.

5. Какие возможны показатели по модулю  $\lambda$  при  $\lambda = 13$ ? Найдите показатель каждого простого числа, меньшего 100. Для каждого показателя, большего 2, разложите первое простое число, которое имеет такой показатель.

## 4.8. Расширение признака делимости

Как и раньше, пусть  $p$  и  $\lambda$  — различные простые числа,  $\lambda > 2$ , и пусть  $f$  — показатель числа  $p$  по модулю  $\lambda$ . В § 4.6 показано, что если  $p$  имеет простой делитель  $h(\alpha)$  среди круговых целых, построенных с помощью корня  $\alpha$  степени  $\lambda$  из единицы, то существует простой способ определить, делится ли данное круговое целое  $a_0 + a_1\eta_1 + \dots + a_e\eta_e$ , образованное периодами длины  $f$ , на  $h(\alpha)$ ; именно, существуют такие целые числа  $u_1, u_2, \dots, u_e$ , что  $a_0 + a_1\eta_1 + \dots + a_e\eta_e$  делится на  $h(\alpha)$  в том и только том случае, когда  $a_0 + a_1u_1 + \dots + a_eu_e \equiv 0 \pmod{p}$ . Иначе говоря,  $\eta_i \equiv u_i \pmod{h(\alpha)}$  и для целых чисел  $x$  сравнение  $x \equiv 0 \pmod{h(\alpha)}$  равносильно сравнению  $x \equiv 0 \pmod{p}$ . В настоящем параграфе мы хотим показать, как расширить этот признак делимости до признака, применимого ко всем круговым целым, а не только к тем, которые образованы периодами длины  $f$ .

Прием, с помощью которого Куммер выполнил такое расширение, основывается на следующей идее, которая восходит к изучению Гауссом деления круга (Disquisitiones Arithmeticae, Art. 348). Пусть  $\eta_0 = \eta_e$  обозначает период  $\alpha + \sigma^e\alpha + \sigma^{2e}\alpha + \dots + \sigma^{-e}\alpha$  длины  $f$ , содержащий  $\alpha$ , и пусть  $P(X)$  — полином от  $X$ , коэффициенты которого являются круговыми целыми и который представляет собой произведение  $\prod (X - \alpha^i)$ , где  $\alpha^i$  пробегает все те степени, которые содержатся в  $\eta_0$ ; иными словами,

$$P(X) = \prod_{i=1}^f (X - \sigma^{ei}\alpha),$$

где, как обычно,  $e = (\lambda - 1)/f$ , а  $\sigma$  есть сопряжение  $\alpha \mapsto \alpha^\gamma$ , определенное примитивным корнем  $\gamma$  по модулю  $\lambda$ . Например, в случае  $\lambda = 13$ ,  $f = 3$  мы имеем  $\eta_0 = \alpha + \alpha^3 + \alpha^{-4}$  и  $P(X) = (X - \alpha)(X - \alpha^3)(X - \alpha^{-4}) = [X^2 - (\alpha + \alpha^3)X + \alpha^4] \times [X - \alpha^{-4}] = X^3 - (\alpha + \alpha^3 + \alpha^{-4})X^2 + (\alpha^4 + \alpha^{-3} + \alpha^{-1})X - 1 = X^3 - \eta_0 X^2 + \eta_2 X - 1$ . (Хотя  $\sigma$  зависит от выбора примитивного корня  $\gamma$ , полином  $P(X)$  зависит только от того, какие степени элемента  $\alpha$  лежат в одном с  $\alpha$  периоде  $\eta_0$ , а это не зависит, как было показано в § 4.5, от выбора  $\gamma$ . Значит, в нашем примере все коэффициенты  $1, -\eta_0, \eta_2, -1$  не должны зависеть от выбора  $\gamma$ . Действительно, для каждого из возможных выборов  $\gamma = \pm 2$  мы имеем  $\eta_2 = \alpha^4 + \alpha^{-3} + \alpha^{-1}$ , тогда как  $\eta_1$  и  $\eta_3$  зависят от выбора  $\gamma$ .) Легко видеть, что во всех случаях, как и в этом, коэффициенты полинома  $P(X)$  являются круговыми целыми, образованными периодами длины  $f$ , т. е.  $P(X)$  имеет вид <sup>1)</sup>  $P(X) = X^f + \varphi_1(\eta)X^{f-1} + \dots + \varphi_{f-1}(\eta)X + \varphi_f(\eta)$ , где  $\varphi_1(\eta), \varphi_2(\eta), \dots, \varphi_f(\eta)$  — круговые целые, образованные периодами длины  $f$ ; для этого достаточно заметить, что  $\sigma^e$  в применении к  $P(X)$  производит только циклическую перестановку сомножителей и, следовательно, оставляет  $P(X)$ , а значит, и все его коэффициенты, без изменения.

Теперь положим  $X = \alpha$ . Так как выражение  $P(\alpha) = \prod (\alpha - \alpha^i)$  содержит множитель  $\alpha - \alpha$ , то это круговое целое есть 0, т. е.

$$\alpha^f + \varphi_1(\eta)\alpha^{f-1} + \dots + \varphi_f(\eta) = 0.$$

Это соотношение будет называться *уравнением для  $\alpha$  над периодами длины  $f$* . В приведенном выше примере оно имеет вид  $\alpha^3 - \eta_0\alpha^2 + \eta_2\alpha - 1 = 0$ . Его можно проверить, выписав периоды:  $\alpha^3 - (\alpha + \alpha^3 + \alpha^9)\alpha^2 + (\alpha^4 + \alpha^{10} + \alpha^{12})\alpha - 1 = \alpha^3 - \alpha^3 - \alpha^5 - \alpha^{11} + \alpha^5 + \alpha^{11} + 1 - 1 = 0$ .

Используя уравнение  $P(\alpha) = 0$  для  $\alpha$  над периодами длины  $f$ , можно представить произвольное круговое целое  $g(\alpha)$  в виде

$$g(\alpha) = g_1(\eta)\alpha^{f-1} + g_2(\eta)\alpha^{f-2} + \dots + g_f(\eta), \quad (1)$$

где  $g_1(\eta), g_2(\eta), \dots, g_f(\eta)$  — круговые целые, образованные периодами длины  $f$ . (Вычислениями можно доказать, что такое представление *единственно*, но этот факт в дальнейшем не понадобится.) Чтобы выполнить это представление, можно последовательно снижать степени  $\alpha$  в  $g(\alpha)$ , пользуясь равенством  $\alpha^f = -\varphi_1(\eta)\alpha^{f-1} - \varphi_2(\eta)\alpha^{f-2} - \dots - \varphi_f(\eta)$ , до тех пор, пока высшая степень элемента  $\alpha$  в  $g(\alpha)$  не станет меньше  $f$ . Этот про-

<sup>1)</sup> Обозначения  $\varphi(\eta), f(\eta), g(\eta)$  и т. д. для круговых целых, образованных периодами, взято у Куммера. Заметим, что они сильно отличаются от обозначения  $f(\alpha)$  в том смысле, что выражение  $f(\eta)$  включает в себя  $e$  различных периодов  $\eta_i$ .



цесс выполняется так же, как процесс деления с остатком для полиномов, т. е. можно писать  $g(\alpha) = q(\alpha)P(\alpha) + r(\alpha)$ , обращаясь с  $g(\alpha)$ ,  $q(\alpha)$ ,  $P(\alpha)$ ,  $r(\alpha)$  как с полиномами от  $\alpha$ , коэффициенты которых являются круговыми целыми, образованными периодами длины  $f$ . (Деление возможно, поскольку старший коэффициент полинома  $P$  равен 1.) Как круговые целые,  $P(\alpha) = 0$  и  $g(\alpha) = r(\alpha)$ , где  $r(\alpha)$  имеет требуемый вид, т. е. является полиномом степени меньше  $f$  и имеет коэффициентами круговые целые, образованные периодами длины  $f$ .

Предположим теперь, что простой делитель  $h(\alpha)$  числа  $p$  задан. Тогда каждый период  $\eta_j$  длины  $f$  сравним по модулю  $h(\alpha)$  с некоторым целым числом  $u_j$ . Следовательно, каждый коэффициент  $g_i(\eta)$  в приведенном выше представлении элемента  $g(\alpha)$  сравним по модулю  $h(\alpha)$  с целым числом  $g_i(u)$ , которое получается из  $g_i(\eta)$  заменой  $\eta_1$  на  $u_1$ ,  $\eta_2$  на  $u_2$ , ...,  $\eta_e$  на  $u_e$ . Более того, так как из сравнимости по модулю  $p$  вытекает сравнимость по модулю  $h(\alpha)$ , то каждое целое число  $g_i(u)$  сравнимо по модулю  $h(\alpha)$  с некоторым неотрицательным целым числом, меньшим  $p$ . Значит, каждое круговое целое  $g(\alpha)$  сравнимо по модулю  $h(\alpha)$  с круговым целым вида  $a_1\alpha^{f-1} + a_2\alpha^{f-2} + \dots + a_f$ , где  $a_i$  — целые числа из промежутка  $0 \leq a_i < p$ . Таким образом, данная задача, заключающаяся в том, чтобы научиться определять, имеет ли место сравнение  $g(\alpha) \equiv 0 \pmod{h(\alpha)}$ , будет решена, если можно будет определить, верно ли сравнение  $a_1\alpha^{f-1} + a_2\alpha^{f-2} + \dots + a_f \equiv 0 \pmod{h(\alpha)}$  именно для этих  $p^f$  конкретных круговых целых. Следовательно, наша задача решается следующей теоремой, устанавливающей, что из этих  $p^f$  круговых целых лишь нуль делится на  $h(\alpha)$ .

**Теорема.** Пусть  $h(\alpha)$  — простой делитель числа  $p$ , где  $p \neq \lambda$  — простое с показателем  $f$  по модулю  $\lambda$ . Пусть  $S$  — множество  $p^f$  круговых целых вида  $a_1\alpha^{f-1} + a_2\alpha^{f-2} + \dots + a_f$ , где  $a_i$  — целые числа из промежутка  $0 \leq a_i < p$ . Тогда описанный выше метод позволяет для любого кругового целого  $g(\alpha)$  найти такое круговое целое  $\bar{g}(\alpha)$  из множества  $S$ , что  $g(\alpha) \equiv \bar{g}(\alpha) \pmod{h(\alpha)}$ . Два элемента из  $S$  сравнимы между собой по модулю  $h(\alpha)$  тогда и только тогда, когда они идентичны. Это дает признак делимости на  $h(\alpha)$ , поскольку оказывается, что для любого  $g(\alpha)$  можно найти такое  $\bar{g}(\alpha)$  из  $S$ , для которого  $g(\alpha) \equiv \bar{g}(\alpha) \pmod{h(\alpha)}$  и при этом  $g(\alpha) \equiv 0 \pmod{h(\alpha)}$  в том и только в том случае, когда  $\bar{g}(\alpha) = 0$ .

**Следствие.** Чтобы определить, делится ли  $g(\alpha)$  на  $h(\alpha)$ , необязательно знать  $h(\alpha)$ ; достаточно знать такие целые числа  $u_1, u_2, \dots, u_e$ , для которых выполняются сравнения  $\eta_i \equiv u_i \pmod{h(\alpha)}$  ( $i = 1, 2, \dots, e$ ).

*Доказательство.* Следствие, конечно, вытекает из того факта, что переход от  $g(\alpha)$  к  $\bar{g}(\alpha)$ , т. е. записывание кругового целого в виде (1) с последующим редуцированием целых чисел  $g_i(u)$  по модулю  $p$ , использует только числа  $u_i$ , но не само  $h(\alpha)$ . Способ доказательства теоремы заключается в простом подсчете, а конкретно в установлении того, что *существуют по крайней мере  $p^f$  не сравнимых по модулю  $h(\alpha)$  круговых целых*. Тогда, так как каждое круговое целое сравнимо с одним из  $p^f$  круговых целых, принадлежащих  $S$ , все  $p^f$  элементов в  $S$  оказываются не сравнимыми по модулю  $h(\alpha)$ , в чем и состоит утверждение теоремы.

Заметим сначала, что число не сравнимых по модулю  $h(\alpha)$  элементов есть степень числа  $p$ , скажем  $p^n$ . В терминах теории групп это непосредственно следует из того, что аддитивная группа круговых целых по модулю  $h(\alpha)$  является факторгруппой аддитивной группы круговых целых по модулю  $p$ , а эта последняя группа содержит  $p^{\lambda-1}$  элементов; число элементов факторгруппы делит  $p^{\lambda-1}$  и, следовательно, поскольку  $p$  просто, должно быть степенью числа  $p$ . Обращения к теории групп легко избежать прямым построением такой системы  $g_1(\alpha), g_2(\alpha), \dots, g_n(\alpha)$  круговых целых, что любое круговое целое сравнимо по модулю  $h(\alpha)$  точно с одним из  $p^n$  круговых целых  $b_1g_1(\alpha) + b_2g_2(\alpha) + \dots + b_ng_n(\alpha)$  ( $0 \leq b_i < p$ ) (см. упр. 4).

Заметим далее, что число не сравнимых по модулю  $h(\alpha)$  круговых целых не меньше  $\lambda + 1$ , поскольку  $0, \alpha, \alpha^2, \dots, \alpha^\lambda = 1$  попарно не сравнимы по модулю  $h(\alpha)$ . Это верно, поскольку норма любого делящегося на  $h(\alpha)$  кругового целого должна делиться на  $p$ , тогда как норма мономов  $\alpha^j - 0$  равна 1, а норма биномов  $\alpha^i - \alpha^j$  ( $i \not\equiv j \pmod{\lambda}$ ) равна  $N(\alpha - 1) = \lambda$ , и ни то, ни другое не делится на  $p$ .

Заметим наконец, что число *ненулевых* не сравнимых по модулю  $h(\alpha)$  круговых целых делится на  $\lambda$ . Это можно доказать следующим образом. Если  $\alpha, \alpha^2, \dots, \alpha^\lambda = 1$  исчерпывают все ненулевые круговые целые по модулю  $h(\alpha)$ , то их точно  $\lambda$ . В противном случае найдется такое круговое целое  $\psi(\alpha)$ , что  $\psi(\alpha) \not\equiv 0 \pmod{h(\alpha)}$  и  $\psi(\alpha) \not\equiv \alpha^j \pmod{h(\alpha)}$  ( $j = 1, 2, \dots, \lambda$ ). Тогда  $\psi(\alpha)\alpha, \psi(\alpha)\alpha^2, \dots, \psi(\alpha)\alpha^\lambda = \psi(\alpha)$  все отличны от нуля по модулю  $h(\alpha)$  (поскольку  $h(\alpha)$  — простое), все различны по модулю  $h(\alpha)$  (поскольку из  $\psi(\alpha)\alpha^j \equiv \psi(\alpha)\alpha^k$  вытекало бы, что  $\alpha^j \equiv \alpha^k$ ) и отличны от  $\alpha, \alpha^2, \dots, \alpha^\lambda$  (поскольку из  $\psi(\alpha)\alpha^j \equiv \alpha^i$  вытекало бы  $\psi(\alpha) \equiv \alpha^k$ ). Если этим мы исчерпали ненулевые круговые целые по модулю  $h(\alpha)$ , то их точно  $2\lambda$ . В противном случае имеется такое круговое целое  $\phi(\alpha)$ , что  $3\lambda$  круговых целых  $\alpha^i, \psi(\alpha)\alpha^j, \phi(\alpha)\alpha^k$  все отличны от нуля и друг от друга по модулю  $h(\alpha)$ . Если этим исчерпаны все возможности, то исследуемое число в точности равно  $3\lambda$ , а в противном случае процесс можно продолжить. В конце концов все возможности будут

исчерпаны и процесс завершится списком из  $m\lambda$  различных ненулевых по модулю  $h(\alpha)$  круговых целых и  $m\lambda = p^n - 1$ .

Таким образом,  $p^n \equiv 1 \pmod{\lambda}$ . По определению показателя  $f$  числа  $p$  по модулю  $\lambda$  это дает  $n \geq f$ . (Заметим, что из  $p^n \geq \lambda + 1$  вытекает, что  $n \neq 0$ .) Итак, число  $p^n$  не сравнимых по модулю  $h(\alpha)$  элементов не меньше  $p^f$ , что и требовалось доказать.

## Упражнения

1. В каждом из следующих случаев найдите уравнение для  $\alpha$  над периодами длины  $f$  и проверьте его непосредственной подстановкой. (a)  $\lambda = 5, f = 2$ . (b)  $\lambda = 7, f = 2$ . (c)  $\lambda = 11, f = 5$ . (d)  $\lambda = 13, f = 3$ . (e)  $\lambda = 31, f = 5$ .

2. Если  $h(\alpha)$  — простой делитель числа  $p$ , для которого известны  $u_i$ , то полином степени  $f$  со старшим коэффициентом 1, который делится на  $h(\alpha)$ , можно найти простой подстановкой чисел  $u_i$  вместо  $\eta_i$  в уравнение для  $\alpha$  над периодами длины  $f$ . Например, в случае  $\lambda = 13, p = 29$  подстановка значений  $u_0 = -3, u_1 = 14, u_2 = 12, u_3 = 5$ , найденных в § 4.7, в уравнение  $\alpha^3 - \eta_0\alpha^2 + \eta_2\alpha - 1 = 0$  из этого параграфа дает в качестве кругового целого, делящегося на  $h(\alpha)$ , о котором идет речь,  $\alpha^3 + 3\alpha^2 + 12\alpha - 1$ . Четыре различных сопряженных этого  $h(\alpha)$  имеют  $u_i$ , получаемые циклическими перестановками из указанных выше. Следовательно, произведение  $(\alpha^3 + 13\alpha^2 + 12\alpha - 1)(\alpha^3 - 14\alpha^2 + 5\alpha - 1)(\alpha^3 - 12\alpha^2 - 3\alpha - 1) \times (\alpha^3 - 5\alpha^2 + 14\alpha - 1)$  делится на все четыре простых делителя числа 29 (если 29 имеет простые делители), и можно ожидать, что оно делится на 29. Докажите это непосредственно, проверив, что это произведение сравнимо с  $\alpha^{12} + \alpha^{11} + \alpha^{10} + \dots + 1 = 0$  по модулю 29. [Перемножьте полиномы.]

3. Технику упр. 2 можно рассматривать как способ *разложения полинома*  $X^{\lambda-1} + X^{\lambda-2} + \dots + X + 1$  по модулю  $p$ . Используя эту технику, разложите  $X^4 + X^3 + X^2 + X + 1$  по модулю 19, по модулю 59 и по модулю 41. Далее разложите  $X^6 + X^5 + \dots + 1$  по модулю 3, по модулю 13, по модулю 29. Наконец, разложите  $X^{30} + X^{29} + \dots + 1$  по модулю 2. В каждом случае отыскивается  $e$  сомножителей степени  $f$ , где  $f$  — показатель числа  $p$  по модулю  $\lambda$ . Как будет вытекать из теоремы следующего параграфа, эти сомножители *неразложимы* по модулю  $p$ .

4. Докажите, что число не сравнимых по модулю  $h(\alpha)$  круговых целых есть степень числа  $p$ . [Целые числа  $0, 1, 2, \dots, p-1$  представляют собой  $p$  не сравнимых по модулю  $h(\alpha)$  элементов, поскольку для целых чисел сравнимость по модулю  $h(\alpha)$  равносильна сравнимости по модулю  $p$ . Если найдется некоторое  $g_1(\alpha)$ , не сравнимое ни с одним из этих элементов, то числа  $a + bg_1(\alpha)$  не сравнимы друг с другом при  $0 \leq a < p, 0 \leq b < p$ . Если на этом все возможности исчерпываются, то ответ  $p^2$ . В противном случае рассуждение можно продолжить и образовать  $p^3$  не сравнимых элементов, и т. д.]

5. Определите, какие из простых чисел табл. 4.7.2 делят  $7\alpha^3 + 45\alpha^2 + 83\alpha + 90$ . [Заметим, что каждая строка таблицы дает *два* простых — то, которое там указано, и его сопряженное.]

6. Покажите, что для каждого простого делителя  $h(\alpha)$  простого числа  $p$  показателя  $f$  по модулю  $\lambda$  имеется полином  $Q_h(\alpha)$  степени  $f$  относительно  $\alpha$  с целыми коэффициентами и со старшим коэффициентом 1, обладающий следующим свойством: круговое целое  $h(\alpha)$  тогда и только тогда делит круговое целое  $g(\alpha)$ , когда деление полиномов  $g(X) = q(X)Q_h(X) + r(X)$  дает остаток  $r(X)$ , все коэффициенты которого сравнимы с нулем по модулю  $p$ .

## 4.9. Простые дивизоры

Пусть  $\lambda$  — простое число, большее 2, и пусть  $p \neq \lambda$  — простое число, показатель которого по модулю  $\lambda$  есть  $f$ . В § 4.6 было показано, что если  $p$  имеет простой делитель  $h(\alpha)$ , т. е. имеется простое круговое целое  $h(\alpha)$ , которое делит число  $p$ , то каждый из  $e (= (\lambda - 1)/f)$  периодов  $\eta_1, \eta_2, \dots, \eta_e$  длины  $f$  сравним по модулю  $h(\alpha)$  с некоторым целым числом. Это означает, что для данного простого делителя  $h(\alpha)$  числа  $p$  существуют целые числа  $u_1, u_2, \dots, u_e$ , для которых  $\eta_i \equiv u_i \pmod{h(\alpha)}$ . Следовательно, любое круговое целое, образованное периодами длины  $f$ , сравнимо по модулю  $h(\alpha)$  с целым числом, и, поскольку два целых числа сравнимы по модулю  $h(\alpha)$  тогда и только тогда, когда они сравнимы по модулю  $p$ , знание целых чисел  $u_i$  дает возможность определять, сравнимы ли по модулю  $h(\alpha)$  два круговых целых, образованных периодами длины  $f$ . Короче говоря, сравнение  $g(\eta) \equiv \varphi(\eta) \pmod{h(\alpha)}$  равносильно<sup>1)</sup> сравнению  $g(u) \equiv \varphi(u) \pmod{p}$ . В частности, из тождеств  $\eta_1 \eta_j = c_0 + c_1 \eta_1 + \dots + c_e \eta_e$  вытекают сравнения  $u_1 u_j \equiv c_0 + c_1 u_1 + \dots + c_e u_e \pmod{p}$  относительно чисел  $u_i$ . Как было видно на примерах из § 4.7, эти сравнения можно решить и найти *все возможные* наборы чисел  $u_i$  в рассматриваемых случаях. Наконец, в § 4.8 было показано, что знание чисел  $u_i$  дает возможность определять, сравнимы ли по модулю  $h(\alpha)$  два круговых целых; если даны  $g(\alpha)$  и  $\varphi(\alpha)$ , то их можно записать в виде  $g(\alpha) = g_1(\eta) \alpha^{f-1} + g_2(\eta) \alpha^{f-2} + \dots + g_f(\eta)$ ,  $\varphi(\alpha) = \varphi_1(\eta) \alpha^{f-1} + \varphi_2(\eta) \alpha^{f-2} + \dots + \varphi_f(\eta)$ , и сравнение  $g(\alpha) \equiv \varphi(\alpha) \pmod{h(\alpha)}$  верно тогда и только тогда, когда верны сравнения  $g_1(u) \equiv \varphi_1(u)$ ,  $g_2(u) \equiv \varphi_2(u)$ ,  $\dots$ ,  $g_f(u) \equiv \varphi_f(u) \pmod{p}$ . Итак, *простой делитель  $h(\alpha)$  числа  $p$  определяет целые числа  $u_1, u_2, \dots, u_e$  по модулю  $p$ , знания которых достаточно для определения отношения сравнимости по модулю  $h(\alpha)$ .*

Основная идея куммеровой теории идеального разложения может быть сформулирована теперь следующим образом. *Доказать, что сравнения по модулю  $p$  относительно  $u_i$  всегда имеют решение, и воспользоваться этим решением для определения «срав-*

<sup>1)</sup> Здесь  $g(u)$  есть целое число, полученное из  $g(\eta)$  заменой  $\eta_i$  на  $u_i$ , и аналогично понимается  $\varphi(u)$ . Как и в § 4.3, этим обозначением нужно пользоваться осторожно, поскольку такая операция на круговых целых, образованных периодами, определена некорректно, т. е. из  $g(\eta) = \varphi(\eta)$  не вытекает  $g(u) = \varphi(u)$ . Однако для тех частных значений  $u_i$ , о которых идет речь, из  $g(\eta) \equiv \varphi(\eta) \pmod{h(\alpha)}$  вытекает  $g(u) \equiv \varphi(u) \pmod{p}$  на основании обычных правил действий со сравнениями по модулю  $h(\alpha)$ , и тем более из  $g(\eta) = \varphi(\eta)$  вытекает  $g(u) \equiv \varphi(u) \pmod{p}$ . Следовательно, несмотря на то, что целые числа  $g(u)$  и  $\varphi(u)$  определены некорректно, они вполне корректно определены *по модулю  $p$*  в случае таких частных значений  $u_i$ .

нимости по модулю простого делителя числа  $p$ » даже в том случае, когда никакого простого делителя числа  $p$  в действительности нет. Это и есть программа данного параграфа. Нашим первым шагом будет следующее

**Предложение.** Пусть заданы  $\lambda, p, f, e$ , как и раньше. Существуют такие целые числа  $u_1, u_2, \dots, u_e$ , что каждое уравнение, которому удовлетворяют периоды  $\eta_i$  длины  $f$ , выполняется как сравнение по модулю  $p$  при подстановке в него целых чисел  $u_i$  вместо периодов  $\eta_i$ . Иными словами,  $u_1, u_2, \dots, u_e$  таковы, что если  $F(\eta_1, \eta_2, \dots, \eta_e)$  — полином от  $\eta_i$  с целыми коэффициентами, а круговое целое  $F(\eta_1, \eta_2, \dots, \eta_e)$  есть нуль, то целое число  $F(u_1, u_2, \dots, u_e)$ , получаемое подстановкой  $u_i$  вместо  $\eta_i$  ( $i = 1, 2, \dots, e$ ), удовлетворяет сравнению  $F(u_1, u_2, \dots, u_e) \equiv 0 \pmod{p}$ .

Если бы было известно, что  $u_i$  возникли из действительно существующего делителя  $h(\alpha)$  числа  $p$ , то техника предыдущего параграфа давала бы право использовать их для определения того, сравнимы ли по модулю  $h(\alpha)$  данные круговые целые. Главная идея как раз в том и заключается, что отношение сравнимости может быть определено даже тогда, когда этого  $h(\alpha)$  на самом деле нет.

**Теорема 1.** Пусть  $\lambda, p, f, e$  и  $u_1, u_2, \dots, u_e$  такие, как в предложении. Тогда можно определить одно и только одно отношение сравнимости для круговых целых с  $\alpha^\lambda = 1$ , для которого выполняются все обычные свойства (оно рефлексивно, симметрично, транзитивно и согласовано со сложением и умножением) и при котором  $\eta_i$  сравнимо с  $u_i$ ,  $p$  сравнимо с 0, а 1 не сравнимо с 0. Кроме того, это отношение сравнимости является простым в том смысле, что произведение сравнимо с 0 только тогда, когда один из сомножителей сравним с нулем. Наконец, число несравнимых элементов в точности равно  $p^f$ .

**Определение.** Отношение сравнимости, существование которого утверждается теоремой 1, будем называть сравнимостью по модулю простого дивизора числа  $p$ , соответствующего набору целых чисел  $u_1, u_2, \dots, u_e$ . Если  $g(\alpha)$  сравнимо с 0 по модулю этого отношения, то будем говорить, что  $g(\alpha)$  делится на простой дивизор числа  $p$ , соответствующий набору  $u_1, u_2, \dots, u_e$ .

Заметим, что «простой дивизор числа  $p$ , соответствующий набору  $u_1, u_2, \dots, u_e$ », не определен, а определена лишь сравнимость по модулю такого дивизора и делимость на такой дивизор. Если  $p$  на самом деле имеет простой делитель  $h(\alpha)$ , то, как было показано, сравнимость по модулю  $h(\alpha)$  совпадает с только что определенной «сравнимостью по модулю простого дивизора чис-



ла  $p$ », а именно, со сравнимостью по модулю простого дивизора числа  $p$ , соответствующего набору  $u_1, u_2, \dots, u_e$ , где  $u_i \equiv \eta_i \pmod{h(\alpha)}$ . Следовательно, новое определение совпадает со старым каждый раз, когда старое определение имеет смысл. Однако новое определение имеет смысл и тогда, когда старое его не имеет. Например, в случае  $\lambda = 23$  сравнимость по модулю простого дивизора числа 47, соответствующего набору  $\alpha \equiv 4, \alpha^2 \equiv 4^2, \dots, \alpha^{22} \equiv 4^{22} \pmod{47}$ , теперь определена, несмотря на то что никакого простого кругового целого  $h(\alpha)$ , делящего число 47, нет. Иногда в тех случаях, когда нет реального простого делителя числа  $p$ , чтобы специально подчеркнуть этот факт, сравнимость по модулю простого дивизора называют сравнимостью по модулю *идеального* простого делителя, а делимость на простой дивизор — делимостью на *идеальный* простой делитель. Однако утверждения, касающиеся сравнимости по модулю простых дивизоров или делимости на простой дивизор, имеют смысл, согласно приведенному определению, и в тех случаях, когда реальных делителей нет.

Если набор целых чисел  $u_1, u_2, \dots, u_e$  обладает свойством, описанным в предложении, то им обладает также набор  $u_2, u_3, \dots, u_e, u_1$  и, следовательно, все  $e$  наборов, получаемых из исходного циклическими перестановками чисел  $u_i$ . Это непосредственно следует из того, что имеется сопряжение  $\alpha \mapsto \alpha^\gamma$ , вызывающее циклическую перестановку  $\eta_1 \mapsto \eta_2 \mapsto \dots \mapsto \eta_e \mapsto \eta_1$  периодов и, следовательно, переводящее соотношение вида  $F(\eta_1, \eta_2, \dots, \eta_e) = 0$  в соотношение  $F(\eta_2, \eta_3, \dots, \eta_e, \eta_1) = 0$ . Таким образом, предложение гарантирует существование не только одного, но  $e$  наборов чисел  $u_i$ . В примерах из § 4.7 мы видели, что всегда имелось *точно*  $e$  решений  $u_1, u_2, \dots, u_e$  и что все они могли быть получены из какого-нибудь одного циклическими перестановками. Кроме того, во всех примерах, кроме одного, было возможно показать, что если  $p$  имеет разложение на простые круговые целые сомножители, то оно обязательно имеет такое разложение вида  $p = \pm \varphi(\eta) \cdot \sigma \varphi(\eta) \cdot \dots \cdot \sigma^{e-1} \varphi(\eta)$ , где  $\varphi(\eta)$  простое, т. е.  $p$  должно быть произведением единицы и  $e$  различных простых сомножителей. Следующая теорема устанавливает, что если эти свойства выразить в терминах делимости на простой дивизор — т. е. в более широком смысле, — то они всегда верны.

**Теорема 2.** Для данных  $\lambda, p, f, e$  пусть  $u_1, u_2, \dots, u_e$  и  $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_e$  — два произвольных набора целых чисел, для которых выполнены свойства, указанные в предложении. Тогда имеется одно и только одно целое число  $k, 0 \leq k < e$ , такое, что сравнимость по модулю простого дивизора числа  $p$ , соответствующего набору  $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_e$ , совпадает со сравнимостью по модулю простого дивизора числа  $p$ , соответствующего набору  $u_{1+k},$



$u_{2+k}, \dots, u_k$ , где, как обычно,  $u_j = u_{j+e}$  по определению. Таким образом, имеется точно  $e$  различных отношений сравнимости типа описанного в теореме 1. Делимость на  $p$  равносильна делимости на каждый из этих  $e$  простых дивизоров числа  $p$ , т. е. круговое целое  $g(\alpha)$  делится на  $p$  в обычном смысле тогда и только тогда, когда оно делится на все  $e$  простых дивизоров числа  $p$  во вновь определенном смысле.

Остальная часть параграфа посвящена доказательству предложения и двух теорем. Эти доказательства являются, по существу, теми доказательствами, которые дал Куммер, но центральная идея построения кругового целого  $\Psi(\eta)$  появилась не в первоначальном трактате [K8] 1847 г. по теории идеального разложения, а в короткой заметке [K16], написанной 10 лет спустя. Любопытно, что первоначальные доказательства Куммера были совершенно неверны и в течение первых 10 лет своего существования куммерова теория стояла на порочной основе. Брешь в важнейшем месте, каковым является доказательство приведенного выше предложения, уже начали замечать другие математики (см. [E3]) около 1856 г., но статья 1857 г. появилась еще до того, как изъян стал хорошо известен. По какой-то причине Куммер не торопился признать эту ошибку в своей работе. Фактически в его первоначальном доказательстве было два пробела: первый — в доказательстве того, что сравнение степени  $e$  от  $u$ , т. е. от каждого из  $u_i$ , имеет  $e$  решений по модулю  $p$  (с учетом кратностей), а второй — в доказательстве того, что эти  $e$  решений можно упорядочить так, что они будут обладать свойствами, описанными в предложении. По поводу первого пробела Куммер все еще настаивал в 1857 г., что в своей ранней работе он привел «строгое доказательство», хотя им не было дано там никакого разъяснения этого «доказательства». Хотя исправить этот первый пробел не очень трудно (см. упр. 6), кажется маловероятным, чтобы это удалось сделать на пути, предложенном Куммером в его весьма сокращенном «доказательстве» (см. упр. 7). Что касается второго пробела, восполнить который, по-видимому, труднее, то здесь Куммер, вероятно, был более защищен и потому сказал, что считает это место требующим «разъяснения и более полного обоснования» и по этой причине предлагает новый метод доказательства. Этот новый метод был безусловно значительно проще и стоил того, чтобы его изложить, даже если Куммер искренне верил, на что он намекал, в безукоризненность раннего метода. Однако кажется более правдоподобным, что он в это время уже осознавал недостатки своего раннего метода, но считал неразумным привлекать к ним внимание.

*Доказательство предложения.* Пусть круговое целое  $\Psi(\eta)$ , образованное периодами длины  $f$ , построено следующим образом.

Рассмотрим  $er$  круговых целых  $j - \eta_i$  ( $j = 1, 2, \dots, r$  и  $i = 1, 2, \dots, e$ ). На первом шаге выберем из этих  $er$  круговых целых одно, которое не делится на  $p$ . (Очевидно (см. упр. 9), что хотя бы одно такое среди них всегда найдется.) На  $n$ -м шаге мы выберем из оставшихся  $er - (n - 1)$  круговых целых  $j - \eta_i$  одно таким способом, чтобы произведение всех  $n$  этих уже выбранных элементов не делилось на  $p$ . Если выбрать  $n$ -й сомножитель с таким свойством невозможно, то конструкция завершена и  $\Psi(\eta)$  определяется как произведение  $(n - 1)$  уже выбранных<sup>1)</sup> к этому моменту сомножителей. Как было показано в § 4.6,  $(\eta_i - 1)(\eta_i - 2) \dots (\eta_i - p) \equiv \eta_i^p - \eta_i \equiv 0 \pmod{p}$ , поэтому построение  $\Psi(\eta)$  завершится раньше, чем будут исчерпаны все  $er$  сомножителей, и для каждого  $i$  по крайней мере один сомножитель  $j - \eta_i$  не войдет в  $\Psi(\eta)$ . Обозначим через  $u_i - \eta_i$  для  $i = 1, 2, \dots, e$  тот сомножитель вида  $j - \eta_i$ , который не входит в  $\Psi(\eta)$ . Тогда  $(u_i - \eta_i) \Psi(\eta) \equiv 0 \pmod{p}$ , так как в противном случае построение  $\Psi(\eta)$  не было бы закончено. С другой стороны, если  $j - \eta_i$  — любой сомножитель этого вида, не вошедший в  $\Psi(\eta)$ , то  $(j - \eta_i) \Psi(\eta) \equiv 0 \equiv (u_i - \eta_i) \Psi(\eta) \pmod{p}$ , откуда  $(j - u_i) \Psi(\eta) \equiv 0 \pmod{p}$ . Если  $j \neq u_i$ , то, поскольку и  $j$ , и  $u_i$  лежат в промежутке  $1 \leq u_i \leq p$ ,  $1 \leq j \leq p$ , разность  $j - u_i$  была бы обратима по модулю  $p$ , скажем  $b(j - u_i) \equiv 1 \pmod{p}$ , откуда  $\Psi(\eta) \equiv b(j - u_i) \Psi(\eta) \equiv 0 \pmod{p}$  вопреки предположению. Следовательно,  $j = u_i$  и  $u_i$  является *единственным* целым числом между 1 и  $p$ , для которого  $u_i - \eta_i$  не входит в  $\Psi(\eta)$ . Таким образом,  $\Psi(\eta)$  состоит точно из  $er - e$  сомножителей, а именно, из всех сомножителей  $j - \eta_i$ , кроме  $u_i - \eta_i$ .

Теперь мы имеем  $\eta_i \Psi(\eta) \equiv u_i \Psi(\eta) \pmod{p}$  для  $i = 1, 2, \dots, e$ . Значит,  $F(\eta_1, \eta_2, \dots, \eta_e) \Psi(\eta) \equiv F(u_1, u_2, \dots, u_e) \times \times \Psi(\eta) \pmod{p}$  для любого полинома  $F(\eta_1, \eta_2, \dots, \eta_e)$  от периодов. Это непосредственно вытекает из согласованности сравнимости по модулю  $p$  со сложением и умножением. В частности, если  $F(\eta_1, \eta_2, \dots, \eta_e) = 0$ , то  $F(u_1, u_2, \dots, u_e) \Psi(\eta) \equiv 0 \pmod{p}$ . Так как  $\Psi(\eta) \not\equiv 0 \pmod{p}$  по построению, то целое число  $F(u_1, u_2, \dots, u_e)$  не обратимо по модулю  $p$ , т. е.  $F(u_1, u_2, \dots, u_e) \equiv 0 \pmod{p}$ . Следовательно, целые числа  $u_1, u_2, \dots, u_e$  обладают требуемым в предложении свойством, и предложение доказано.

<sup>1)</sup> Это место слегка отличается от подлинной конструкции Куммера. Вместо того чтобы использовать все  $er$  указанных выше сомножителей, он пользовался только теми сомножителями  $j - \eta_i$ , в которых  $j$  удовлетворяет сравнению  $(j - \eta_1)(j - \eta_2) \dots (j - \eta_e) \equiv 0 \pmod{p}$ . Если бы речь шла о действительном вычислении значения  $\Psi(\eta)$ , то этот способ был бы более эффективным. Однако здесь нашим результатом должно быть не  $\Psi(\eta)$ , а существование целых чисел  $u_i$ . Когда их существование уже известно, то есть много более легких способов нахождения их, чем эта конструкция.

**Доказательство теоремы 1.** Для доказательства удобно считать, что целые числа  $u_1, u_2, \dots, u_e$  не только обладают указанным в предложении свойством, но и получены конструкцией, примененной в доказательстве предложения, включая и то, что круговое целое  $\Psi(\eta)$ , являющееся произведением  $e$  сомножителей  $j - \eta_i$  с условием  $j \neq i$ , не делится на  $p$ . В доказательстве теоремы 2 будет показано, что любой другой набор целых чисел  $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_e$ , для которого выполнены условия предложения, получается из первого набора циклической перестановкой и, следовательно, обладает тем же свойством. Способ доказательства теоремы 1 будет сводиться к тому, чтобы показать, что отношение сравнимости  $g(\alpha) \Psi(\eta) \equiv \varphi(\alpha) \Psi(\eta) \pmod{p}$  удовлетворяет условиям теоремы. Пусть, таким образом, для круговых целых  $g(\alpha)$ ,  $\varphi(\alpha)$  сравнение  $g(\alpha) \equiv \varphi(\alpha)$  означает, что  $g(\alpha) \Psi(\eta) \equiv \varphi(\alpha) \Psi(\eta) \pmod{p}$ . Тогда ясно, что отношение  $\equiv$  рефлексивно, симметрично, транзитивно и согласовано со сложением и умножением. Кроме того,  $p \equiv 0$  и, как видно из доказательства предложения,  $\eta_i \equiv u_i$ . Так как  $\Psi(\eta) \not\equiv 0 \pmod{p}$ , то  $1 \not\equiv 0$ .

Пусть теперь  $\sim$  обозначает любое другое отношение сравнимости, которое рефлексивно, симметрично, транзитивно и согласовано со сложением и умножением и для которого  $\eta_i \sim u_i$ ,  $p \sim 0$ ,  $1 \not\sim 0$ . Из того что каждое круговое целое  $g(\alpha)$  может быть записано в виде  $g_1(\eta) \alpha^{f-1} + g_2(\eta) \alpha^{f-2} + \dots + g_f(\eta)$ , следует, что  $g(\alpha) \sim a_1 \alpha^{f-1} + a_2 \alpha^{f-2} + \dots + a_f$ , где  $a_i$  — целые числа,  $0 \leq a_i < p$ . Значит, имеется самое большее  $p^f$  круговых целых, не сравнимых по отношению  $\sim$ . Покажем, что отношение  $\sim$  должно быть простым и иметь не меньше  $p^f$  несравнимых круговых целых. Отсюда будет вытекать, что отношение  $\sim$  вполне определено, поскольку для любых заданных  $g(\alpha)$  и  $\varphi(\alpha)$  можно добиться выполнения сравнений  $g(\alpha) \sim a_1 \alpha^{f-1} + a_2 \alpha^{f-2} + \dots + a_f$  и  $\varphi(\alpha) \sim b_1 \alpha^{f-1} + b_2 \alpha^{f-2} + \dots + b_f$ , где целые  $a_i$  и  $b_i$  лежат в интервале  $0 \leq a_i, b_i < p$ , а тогда из транзитивности отношения  $\sim$  и из того, что оно имеет  $p^f$  несравнимых круговых целых, будет следовать, что сравнение  $g(\alpha) \sim \varphi(\alpha)$  имеет место в том и только том случае, когда круговые целые  $a_1 \alpha^{f-1} + a_2 \alpha^{f-2} + \dots + a_f$  и  $b_1 \alpha^{f-1} + b_2 \alpha^{f-2} + \dots + b_f$  равны. Так как отношение  $\equiv$  обладает всеми свойствами, которыми, по предположению, обладает отношение  $\sim$ , то эти отношения совпадают, и первое утверждение теоремы будет доказано.

Если бы было показано, что отношение  $\sim$  простое <sup>1)</sup>, то из рассуждений предыдущего параграфа следовало бы, что имеется

<sup>1)</sup> Отношение сравнимости предыдущего параграфа было простым по предположению, поскольку это была сравнимость по модулю  $h(\alpha)$ , где  $h(\alpha)$  — простой делитель числа  $p$ . Смысл теорем этого параграфа в том, чтобы исключить предположение о существовании такого  $h(\alpha)$ .

по крайней мере  $p^f$  не сравнимых по модулю  $\sim$  круговых целых. Действительно, как и раньше, число несравнимых круговых целых было бы степенью числа  $p$  (поскольку речь идет о фактор-группе группы, содержащей  $p^{\lambda-1}$  элементов), большей чем 1 (поскольку  $1 \not\sim 0$ ), которая сравнима с 1 по модулю  $\lambda$  (поскольку подмножества вида  $\{g(\alpha), g(\alpha)\alpha, g(\alpha)\alpha^2, \dots, g(\alpha)\alpha^{\lambda-1}\}$  не перекрывают друг друга и содержат точно  $\lambda$  не сравнимых между собой и с нулем круговых целых); значит, это число есть степень с положительным показателем числа  $p^f$  и оно не меньше  $p^f$ . Следовательно, не только первое утверждение, но и вся теорема будет доказана, если доказать, что отношение  $\sim$  простое.

Способ доказательства будет следующий. Мы покажем, что если отношение  $\sim$  не простое, то имеется другое отношение сравнимости, обозначим его  $\approx$ , которое обладает всеми свойствами отношения  $\sim$ , но которое *грубее*, чем  $\sim$ , т. е. из  $g(\alpha) \sim \varphi(\alpha)$  следует  $g(\alpha) \approx \varphi(\alpha)$ , но имеются такие круговые целые  $g(\alpha)$ ,  $\varphi(\alpha)$ , для которых  $g(\alpha) \approx \varphi(\alpha)$  и  $g(\alpha) \not\sim \varphi(\alpha)$ . Теорема будет следовать из бесконечного спуска: если отношение  $\approx$  не простое, то, поскольку оно обладает всеми свойствами отношения  $\sim$ , процесс можно повторить и получить третье отношение сравнимости  $\approx_3$ , более грубое, чем  $\approx$ , но обладающее всеми свойствами  $\sim$ . Если  $\approx_3$  не простое, то существует четвертое отношение  $\approx_4$ , более грубое, чем  $\approx_3$ , и т. д. Так как число несравнимых круговых целых было не больше  $p^f$  вначале процесса и убывает с каждым шагом, то этот процесс должен привести к отношению сравнимости  $\approx_n$ , обладающему всеми свойствами отношения  $\sim$ , но *вдобавок простому*. Тогда на основании рассуждений предыдущего параграфа, которые были подытожены выше, имеется по крайней мере  $p^f$  не сравнимых по  $\approx_n$  круговых целых. Следовательно, огрубление первоначального отношения  $\sim$  было в действительности невозможно, и это отношение простое и имеет  $p^f$  несравнимых круговых целых.

Таким образом, доказательство теоремы сведено к тому, чтобы показать, что если отношение  $\sim$  не простое, то имеется более грубое отношение сравнимости  $\approx$  с теми же свойствами, что и  $\sim$ . А в этом легко убедиться следующим образом. Если отношение  $\sim$  не простое, то имеются такие круговые целые  $\psi_1(\alpha)$ ,  $\psi_2(\alpha)$ , что  $\psi_1(\alpha)\psi_2(\alpha) \sim 0$ , но  $\psi_1(\alpha) \not\sim 0$ ,  $\psi_2(\alpha) \not\sim 0$ . Пусть запись  $g(\alpha) \approx \varphi(\alpha)$  по определению означает, что  $g(\alpha)\psi_1(\alpha) \sim \varphi(\alpha)\psi_1(\alpha)$ . Тогда отношение  $\approx$  рефлексивно, симметрично, транзитивно и согласовано со сложением и умножением,  $\eta_i \approx u_i$  (поскольку  $\eta_i \sim u_i$  дает  $\eta_i\psi_1(\alpha) \sim u_i\psi_1(\alpha)$ ) и  $p \approx 0$ . Кроме того,  $1 \not\approx 0$ , поскольку  $\psi_1(\alpha) \not\sim 0$ , и отношение  $\approx$  грубее отношения  $\sim$ , поскольку  $\psi_2(\alpha) \approx 0$ , но  $\psi_2(\alpha) \not\sim 0$ . Это завершает доказательство теоремы.

**Доказательство теоремы 2.** Пусть  $u_1, u_2, \dots, u_e$  — набор целых чисел, полученный конструкцией, примененной в доказательстве предложения, и пусть  $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_e$  — любой набор целых чисел, удовлетворяющий условиям предложения. Для доказательства первого утверждения теоремы 2 достаточно доказать, что для этого конкретного набора  $u_1, u_2, \dots, u_e$  имеется единственное целое число  $k$ ,  $0 \leq k < e$ , такое, что  $\bar{u}_i \equiv u_{i+k} \pmod{p}$ , поскольку этим будет доказано, что условиям предложения удовлетворяют только те наборы целых чисел  $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_e$ , которые являются циклическими перестановками набора чисел  $u_i$ ; тогда, так как две циклические перестановки одного и того же множества являются циклическими перестановками друг друга, мы получим требуемое утверждение.

Утверждение этой теоремы о единственности состоит в том, что для каждого  $k = 1, 2, \dots, e - 1$  имеется такое  $i = 1, 2, \dots, e$ , при котором  $u_i \not\equiv u_{i+k} \pmod{p}$ , где, как обычно,  $u_i = u_{i+e}$  по определению; короче, никакая циклическая перестановка, кроме тождественной, не оставляет набор чисел  $u_i$  неизменным по модулю  $p$ . Это — центральное место теоремы. Оно может быть доказано следующим образом.

Рассмотрим конкретные уравнения, которым удовлетворяют периоды. Они имеют вид  $\eta_1 \eta_i = c_0 + c_1 \eta_1 + c_2 \eta_2 + \dots + c_e \eta_e$ . Подсчитывая коэффициенты  $c_j$ , мы просто выписываем все  $f^2$  слагаемых, из которых состоит произведение в левой части, и замечаем, что, так как это произведение инвариантно относительно сопряжения  $\sigma^e$ , то две степени элемента  $\alpha$ , лежащие в одном и том же периоде  $\eta_k$ , должны встречаться одинаковое число раз; это число и есть  $c_k$ . Отсюда видно, что  $f^2 = c_0 + c_1 f + c_2 f + \dots + c_e f$ , поскольку подсчитать число слагаемых в произведении можно двумя способами. Отметим теперь, что  $c_0 \neq 0$  только тогда, когда по крайней мере одно из слагаемых  $\alpha^\mu$  периода  $\eta_i$  обратно к некоторому слагаемому  $\alpha^{-\mu}$  периода  $\eta_1$ . Но в этом случае  $\eta_i$  содержит обратный элемент  $\sigma^{ve} \alpha^\mu$  к каждому слагаемому  $\sigma^{ev} \alpha^{-\mu}$  периода  $\eta_1$ . Следовательно,  $c_0 = f$  для одного этого значения  $j$  и  $c_0 = 0$  для всех других значений  $j$ . Тогда для одного значения  $j$  имеем  $c_0 = f$ ,  $c_1 + c_2 + \dots + c_e = (f^2 - f)/f = f - 1$ , в то время как для всех остальных  $c_0 = 0$ ,  $c_1 + c_2 + \dots + c_e = f$ . (В действительности можно точно сказать, какое значение  $j$  является таким исключительным. Именно,  $j = 0$ , если  $f$  четно, и  $j = e/2$ , если  $j$  нечетно; см. упр. 11. Однако нам это не потребуется.) Значит,  $\eta_1 \eta_j + \eta_2 \eta_{j+1} + \dots + \eta_e \eta_{j-1} = \eta_1 \eta_j + \sigma(\eta_1 \eta_j) + \dots + \sigma^{e-1}(\eta_1 \eta_j) = e c_0 + c_1(\eta_1 + \eta_2 + \dots + \eta_e) + \dots + c_e(\eta_e + \eta_1 + \dots + \eta_{e-1}) = e c_0 - (c_1 + c_2 + \dots + c_e) = -f$  во всех случаях, кроме одного; в этом исключительном случае  $ef - (f - 1) = ef + 1 - f = \lambda - f$ . Тем самым доказано по-



лезное тождество

$$f + \eta_1 \eta_j + \eta_2 \eta_{j+1} + \dots + \eta_e \eta_{j-1} = \begin{cases} \lambda & \text{в одном случае,} \\ 0 & \text{во всех остальных случаях.} \end{cases}$$

Следовательно, согласно определяющему свойству для чисел  $u_i$ ,

$$f + u_1 u_j + u_2 u_{j+1} + \dots + u_e u_{j-1} \begin{cases} \not\equiv 0 \pmod{p} & \text{в одном случае,} \\ \equiv 0 \pmod{p} & \text{во всех остальных случаях.} \end{cases}$$

Если бы существовало такое  $k$ , что  $u_i \equiv u_{i+k} \pmod{p}$  для всех  $i$ , то было бы  $f + u_1 u_j + u_2 u_{j+1} + \dots + u_e u_{j-1} \equiv f + u_1 u_{j+k} + u_2 u_{j+k+1} + \dots + u_e u_{j+k-1} \pmod{p}$ ; если  $j$  принимает то единственное значение, при котором целое число в левой части отлично от нуля по модулю  $p$ , то из этого сравнения вытекает сравнение  $j \equiv j + k \pmod{e}$ , т. е.  $k \equiv 0 \pmod{e}$ , что и требовалось доказать.

Этим доказано, что  $e$  циклических перестановок чисел  $u_i$  все различны. Теперь рассмотрим  $M = \Psi(\eta) + \sigma\Psi(\eta) + \dots + \sigma^{e-1}\Psi(\eta)$ , где  $\sigma$  — сопряжение  $\alpha \mapsto \alpha^\nu$ , переводящее  $\eta_i$  в  $\eta_{i+1}$ . Так как  $\sigma M = M$ , то ясно, что  $M$  — обычное целое число. Далее,

$$\begin{aligned} M\Psi(\eta) &= \Psi(\eta)\Psi(\eta) + [\sigma\Psi(\eta)]\Psi(\eta) + \dots + [\sigma^{e-1}\Psi(\eta)]\Psi(\eta) \equiv \\ &\equiv \Psi(u)\Psi(\eta) + [\sigma\Psi(u)]\Psi(\eta) + \dots + [\sigma^{e-1}\Psi(u)]\Psi(\eta) \pmod{p}, \end{aligned}$$

где через  $\sigma^k\Psi(u)$  обозначено целое число, получаемое действием сопряжения  $\sigma^k$  на  $\Psi(\eta)$  с последующей подстановкой  $\eta_1 = u_1$ ,  $\eta_2 = u_2$ ,  $\dots$ ,  $\eta_e = u_e$  в результат; короче,  $\sigma^k\Psi(u) = \Pi(j - u_{i+k})$ , где  $i = 1, 2, \dots, e$ , а  $j$  пробегает все целые значения от 1 до  $p$ , кроме  $u_i$ . На основании уже доказанного,  $\sigma^k\Psi(u)$  содержит сомножитель, равный 0 (а именно, сомножитель  $u_{i+k} - u_i$ ), для всех  $k$ , кроме  $k = 0$ , а в последнем случае  $\sigma^k\Psi(u) = \Psi(u)$ . Значит,  $M\Psi(\eta) \equiv \Psi(u)\Psi(\eta) \not\equiv 0 \pmod{p}$ , поскольку  $\Psi(u) \not\equiv 0 \pmod{p}$ . [ $\Psi(u)$  есть произведение  $ep - e$  целых чисел, ни одно из которых не делится на  $p$ .] Следовательно,  $M \not\equiv 0 \pmod{p}$ .

Если  $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_e$  удовлетворяют условию предложения, то  $M \equiv \Psi(\bar{u}) + \sigma\Psi(\bar{u}) + \dots + \sigma^{e-1}\Psi(\bar{u}) \pmod{p}$ . Так как  $M \not\equiv 0 \pmod{p}$ , то это дает  $\sigma^k\Psi(\bar{u}) \not\equiv 0 \pmod{p}$  для по крайней мере одного  $k$ . Это означает, что  $\Pi(j - \bar{u}_{i+k}) \not\equiv 0 \pmod{p}$  для по крайней мере одного  $k$ , где  $i = 1, 2, \dots, e$ , а  $j$  принимает любые значения из  $1, 2, \dots, p$ , кроме  $u_i$ . Отсюда вытекает, что  $u_i \equiv \bar{u}_{i+k} \pmod{p}$ , и набор чисел  $\bar{u}_i$  оказывается циклической перестановкой набора чисел  $u_i$ , что и требовалось доказать.

Наконец, остается показать, что сравнение  $g(\alpha) \equiv 0 \pmod{p}$  равносильно тому, что  $g(\alpha)$  делится на все  $e$  простых дивизоров,



которые были определены. Так как  $p$  делится на все  $e$  из них, то половина этого утверждения следует из того, что сравнимость по простому дивизору согласована с умножением. Обратно, как показано в доказательстве теоремы 1, делимость кругового целого  $g(\alpha)$  на простой дивизор числа  $p$ , соответствующий набору  $u_1, u_2, \dots, u_e$ , равносильна сравнению  $g(\alpha) \Psi(\eta) \equiv 0 \pmod{p}$ , где  $\Psi(\eta)$  есть произведение  $e p - e$  сомножителей  $j - \eta_i$ , в которых  $j \neq u_i$ . Значит, делимость элемента  $g(\alpha)$  на простой дивизор числа  $p$ , соответствующий набору  $u_{k+1}, u_{k+2}, \dots, u_k$ , равносильна сравнению  $g(\alpha) \sigma^{-k} \Psi(\eta) \equiv 0 \pmod{p}$ , поскольку

$$\begin{aligned} \sigma^{-k} \Psi(\eta) &= \sigma^{-k} \left[ \prod_{i=1}^e \prod_{j=1}^p (j - \eta_i) / \prod_{i=1}^e (u_i - \eta_i) \right] = \\ &= \prod_{i=1}^e \prod_{j=1}^p (j - \eta_{i-k}) / \prod_{i=1}^e (u_i - \eta_{i-k}) = \\ &= \prod_{i=1}^e \prod_{j=1}^p (j - \eta_i) / \prod_{i=1}^e (u_{i+k} - \eta_i), \end{aligned}$$

т. е.  $\sigma^{-k} \Psi(\eta)$  получается из  $\Psi(\eta)$  заменой  $u_1, u_2, \dots, u_e$  на  $u_{1+k}, u_{2+k}, \dots, u_k$ . Следовательно, если  $g(\alpha)$  делится на все  $e$  простых дивизоров числа  $p$ , то  $g(\alpha) \sigma^{-k} \Psi(\eta) \equiv 0 \pmod{p}$  для всех  $k = 0, 1, \dots, e - 1$ . Суммирование этих сравнений дает  $g(\alpha) \cdot M \equiv 0 \pmod{p}$ , откуда, благодаря тому что  $M \not\equiv 0 \pmod{p}$ , вытекает  $g(\alpha) \equiv 0 \pmod{p}$ , что и требовалось доказать.

## Упражнения

1. Постройте  $\Psi(\eta)$  по модулю 2 для простого дивизора числа 2 в случае  $\lambda = 31$ , который был найден в § 4.7. [Конечно, для доказательств данного параграфа необходимо знать  $\Psi(\eta)$  только по модулю  $p$ .]

2. Постройте  $\Psi(\eta)$  по модулю 3 для простого дивизора числа 3 в случае  $\lambda = 13$ , найденного в § 4.7.

3. Докажите, что если  $p$  имеет показатель  $\lambda - 1$  по модулю  $\lambda$ , то  $p$  — простое круговое целое. [Это сводится главным образом к проверке того, что доказательства этого параграфа справедливы при  $e = 1$ .]

4. Докажите, что сомножители, найденные в примерах из § 4.7 (т. е. круговые целые  $\varphi(\eta)$ , образованные периодами длины  $f$ , имеющие норму  $p^f$ , где  $p$  — простое число с показателем  $f$  по модулю  $\lambda$ ), являются простыми. [Одно из возможных доказательств дано в § 4.11.]

5. Покажите, что если  $\eta_1, \eta_2, \dots, \eta_e$  суть  $e$  периодов длины  $f$  ( $ef = \lambda - 1$ ), то  $\varphi(X) = (X - \eta_1)(X - \eta_2) \dots (X - \eta_e)$  является полиномом от  $X$  с целыми коэффициентами. Найдите этот полином во всех случаях при  $\lambda \leq 13$ .

6. Первым шагом данного Куммером ошибочного «доказательства» предложения была попытка показать, что полином  $\varphi(X)$  из упр. 5 таков, что сравнение  $\varphi(u) \equiv 0 \pmod{p}$  имеет  $e$  различных по модулю  $p$  решений.

Правильное доказательство этого факта может быть дано следующим образом. Имеем

$$\begin{aligned} \varphi(X-1)\varphi(X-2)\cdots\varphi(X-p) &\equiv \\ &\equiv [(X-\eta_1)^p - (X-\eta_1)] [(X-\eta_2)^p - (X-\eta_2)] \cdots [(X-\eta_e)^p - (X-\eta_e)] \equiv \\ &\equiv (X-1)^e (X-2)^e \cdots (X-p)^e \pmod{p} \end{aligned}$$

Следовательно,  $\varphi(X)$  является произведением по модулю  $p$  сомножителей вида  $X - k$  ( $k$  — целое число), и в этом заключается смысл утверждения, что  $\varphi(X)$  имеет  $e$  различных корней по модулю  $p$ . Восполните детали этого доказательства, обращая особое внимание на определение понятия двух совпадающих корней сравнения  $g(u) \equiv 0 \pmod{p}$ .

7. Куммер в «доказательстве» утверждения из упр. 6 говорит, что для каждого целого  $y$  имеют место сравнения  $(y - \eta_i - 1)(y - \eta_i - 2) \cdots (y - \eta_i - p) \equiv (y - \eta_i)^p - (y - \eta_i) \equiv (y^p - y) - (\eta_i^p - \eta_i) \equiv y^p - y \equiv 0 \pmod{p}$ , откуда  $\varphi(y-1)\varphi(y-2)\cdots\varphi(y-p) \equiv 0 \pmod{p^e}$ ; затем он говорит: «легко видеть», что сравнение  $\varphi(y) \equiv 0 \pmod{p}$  имеет  $e$  различных решений. Опровергните это утверждение, найдя такие числа  $p$ ,  $e$  и полином  $\varphi(X)$ , что  $\varphi(y-1)\varphi(y-2)\cdots\varphi(y-p) \equiv 0 \pmod{p^e}$  для всех целых  $y$ , но степень полинома  $\varphi(y)$  меньше  $e$ . [Можно взять  $p = 2$ ,  $e = 3$ .]

8. В примерах из § 4.7 (и из § 4.4) основным шагом в построении простого делителя было нахождение одного решения  $u$  сравнения  $\varphi(u) \equiv 0 \pmod{p}$ , после чего было нетрудно найти остальные  $e - 1$  решений и их точный порядок. Выясните, какие вычислительные обстоятельства делали это возможным и могли бы понадобиться для того, чтобы перейти от одного решения сравнения  $\varphi(u) \equiv 0$  к полному набору чисел  $u_i$ , обладающих свойствами из предложения. [Если  $u_0$  известно, то  $u_1, u_2, \dots, u_{e-1}$  удовлетворяют  $e - 1$  линейным сравнениям с  $e - 1$  неизвестными. Свойства решений таких сравнений похожи на свойства решений линейных уравнений. Это дает *необходимые* условия для наборов чисел  $u_i$ , но, даже если они выполнены, еще неясно, что эти наборы обладают *всеми* требуемыми свойствами.] Здесь была вторая брешь в первоначальном «доказательстве» Куммера.

9. Покажите, что по крайней мере одно из  $ep$  круговых целых  $j - \eta_i$  ( $j = 1, 2, \dots, p$  и  $i = 1, 2, \dots, e$ ) не делится на  $p$ .

10. На современном алгебраическом языке построение простого дивизора числа  $p$  сводится к построению поля из  $p^f$  элементов и гомоморфизма множества круговых целых в это поле, а это в свою очередь сводится к построению полинома степени  $f$ , неразложимого по модулю  $p$ , который делит по модулю  $p$  полином  $X^{p^f-1} + X^{p^f-2} + \dots + X + 1$ , определяющий круговые целые. Выполните это построение с самого начала. Найдите полиномы в случае простых делителей, построенных в § 4.4 и 4.7. [См. упр. 2 и 3 к § 4.8.]

11. Пусть целое число  $j$  лежит в промежутке  $0 \leq j < e$ , и пусть для него элемент  $\alpha^{-1}$  лежит в  $\eta_j$ . Покажите, что  $j = 0$ , если  $f$  четно, и  $j = e/2$ , если  $f$  нечетно.

#### 4.10. Кратности и исключительное простое число

Целью куммеровой теории идеального разложения было «спасение» свойства единственности разложения на простые для круговых целых. Если задачу сформулировать вкратце, то требовалось

показать, что с точностью до сомножителя, являющегося единицей, круговое целое определяется своими простыми дивизорами. Основной объем работы, нужной для осуществления этой цели, содержится в предыдущем параграфе, где понятие «простого дивизора» расширено настолько, чтобы включить в него случаи, когда делимость на простой дивизор нельзя отождествить с делимостью на реально существующее круговое целое. Однако эти определения должны быть дополнены в двух направлениях — одном очень важном и втором не столь значительном, — прежде чем может быть развита полная теория. Важное дополнение — это понятие *кратности*, с которой данный простой дивизор делит данное круговое целое. Ведь даже для обычных положительных целых чисел неверно, что целое число определено своими простыми делителями. Однако оно определено своими простыми делителями и кратностями, с которыми оно делится на каждый из них. (Например, числа  $12 = 2^2 \cdot 3$  и  $18 = 2 \cdot 3^2$  имеют одинаковые простые делители.) Второе, более мелкое дополнение состоит в том, что необходимо изучить простые дивизоры самого числа  $\lambda$  — единственного простого целого числа, не охваченного теоремами предыдущего параграфа.

Если делимость на простой дивизор числа  $p$  совпадает с делимостью на реальное круговое целое  $h(\alpha)$ , то легко приписать кратности. Пусть  $g(\alpha)$  делится на такой простой дивизор; тогда мы можем выполнить деление на  $h(\alpha)$  и найти частное  $g(\alpha)/h(\alpha)$ , являющееся круговым целым. Если это частное снова делится на  $h(\alpha)$ , то можно снова выполнить деление и найти  $g(\alpha)/h(\alpha)^2$ , и т. д. При этом говорят, что  $g(\alpha)$  делится  $\mu$  раз на рассматриваемый простой дивизор, если  $g(\alpha)$  делится на  $h(\alpha)^\mu$ . Однако если никакого реального  $h(\alpha)$  нет, то нужно придумать какой-то другой способ определения кратностей. Идея, которая лежит в основе следующего определения, состоит в том, что круговое целое  $\Psi(\eta)$ , использованное в конструкции предыдущего параграфа, делится на все простые дивизоры числа  $p$ , *кроме* одного — рассматриваемого. Таким образом, круговое целое  $g(\alpha)$ , умноженное на достаточно высокую степень  $\Psi(\eta)$ , будет делиться на  $p$  столько раз, сколько раз  $g(\alpha)$  делится на простой дивизор числа  $p$ , отсутствующий в  $\Psi(\eta)$ .

**Определение.** Говорят, что круговое целое  $g(\alpha)$  делится  $\mu$  раз на простой дивизор числа  $p$ , соответствующий набору  $u_1, u_2, \dots, u_e$ , если  $g(\alpha) \Psi(\eta)^\mu$  делится на  $p^\mu$ , где  $\Psi(\eta)$  — произведение  $e p$  —  $e$  сомножителей  $j - \eta_i$  ( $i = 1, 2, \dots, e; j = 0, 1, \dots, p - 1; j \neq u_i$ ), не делящихся на этот простой дивизор. Говорят, что оно делится на этот простой дивизор *точно*  $\mu$  раз, если оно делится на него  $\mu$  раз, но не делится  $\mu + 1$  раз.

**Предложение.** Понятие «делится один раз» совпадает с понятием «делится», определенным в предыдущем параграфе. Понятие «делится точно нуль раз» совпадает с понятием «не делится». Число  $p$  делится точно один раз, а число 1 не делится на рассматриваемый простой дивизор. Если  $g_1(\alpha)$  и  $g_2(\alpha)$  оба делятся  $\mu$  раз, то это же можно сказать и о  $g_1(\alpha) + g_2(\alpha)$ . Если  $g_1(\alpha)$  делится точно  $\mu$  раз, а  $g_2(\alpha)$  делится точно  $\nu$  раз, то  $g_1(\alpha) g_2(\alpha)$  делится точно  $\mu + \nu$  раз. Наконец, если  $g(\alpha) \neq 0$ , то имеется единственное целое число  $\mu \geq 0$ , такое, что  $g(\alpha)$  делится точно  $\mu$  раз.

**Доказательство.** В предыдущем параграфе было показано, что  $g(\alpha)$  тогда и только тогда делится на простой дивизор, когда  $g(\alpha) \Psi(\eta) \equiv 0 \pmod{p}$ , т. е. когда  $g(\alpha)$  делится один раз. Это доказывает первые два утверждения предложения. Третье утверждение означает, что  $p^2$  не делит  $p[\Psi(\eta)]^2$ , или, что то же самое,  $\Psi(\eta) \Psi(\eta) \not\equiv 0 \pmod{p}$ . Это доказано в предыдущем параграфе. Утверждение, что число 1 не делится на простой дивизор, в точности совпадает с утверждением, что  $\Psi(\eta) \not\equiv 0 \pmod{p}$ .

Следующее утверждение — что  $g_1(\alpha) + g_2(\alpha)$  делится  $\mu$  раз, когда  $g_1(\alpha)$  и  $g_2(\alpha)$  делятся  $\mu$  раз, — непосредственно следует из определения. Далее, если  $g_1(\alpha)$  делится точно  $\mu$  раз, то  $g_1(\alpha) \Psi(\eta)^\mu$  делится на  $p^\mu$ , но  $g_1(\alpha) \Psi(\eta)^{\mu+1}$  не делится на  $p^{\mu+1}$ . Следовательно,  $\varphi_1(\alpha) = p^{-\mu} g_1(\alpha) \Psi(\eta)^\mu$  есть круговое целое. Если бы  $\varphi_1(\alpha)$  делилось на рассматриваемый простой дивизор, то, так как  $\Psi(\eta)$  делится на остальные  $e - 1$  простых дивизоров числа  $p[\Psi(\eta) \sigma^k \Psi(\eta) \equiv 0 \pmod{p}]$ , отсюда следовало бы, что  $\varphi_1(\alpha) \Psi(\eta)$  делится на все  $e$  простых дивизоров числа  $p$ ; значит, по теореме предыдущего параграфа, отсюда вытекало бы, что  $p$  делит  $\varphi_1(\alpha) \Psi(\eta)$ , а значит,  $g_1(\alpha)$  делится  $\mu + 1$  раз на рассматриваемый простой дивизор вопреки предположенному. Следовательно,  $\varphi_1(\alpha)$  не делится на рассматриваемый простой дивизор. Аналогично, если  $g_2(\alpha)$  делится точно  $\nu$  раз, то  $\varphi_2(\alpha) = p^{-\nu} g_2(\alpha) \Psi(\eta)^\nu$  есть круговое целое, не делящееся на рассматриваемый простой дивизор числа  $p$ . Следовательно,  $g_1(\alpha) g_2(\alpha) \Psi(\eta)^{\mu+\nu}$  делится на  $p^{\mu+\nu}$  и частное есть произведение  $\varphi_1(\alpha) \varphi_2(\alpha)$  двух круговых целых, ни одно из которых не делится на рассматриваемый простой дивизор. Поскольку этот простой дивизор прост,  $\varphi_1(\alpha) \varphi_2(\alpha)$  не делится на рассматриваемый простой дивизор. Так как  $\Psi(\eta)$  не делится на этот простой дивизор [ $\Psi(\eta) \Psi(\eta) \not\equiv 0 \pmod{p}$ ], то отсюда вытекает, что произведение  $\varphi_1(\alpha) \varphi_2(\alpha) \Psi(\eta) = g_1(\alpha) g_2(\alpha) \Psi(\eta)^{\mu+\nu+1} p^{-\mu-\nu}$  не делится на простой дивизор числа  $p$  и тем более не делится на  $p$ . Следовательно,  $g_1(\alpha) g_2(\alpha) \times \times \Psi(\eta)^{\mu+\nu+1}$  не делится на  $p^{\mu+\nu+1}$ , а значит,  $g_1(\alpha) g_2(\alpha)$  делится с кратностью точно  $\mu + \nu$ , что и требовалось установить.

Пусть  $g(\alpha)$  — данное круговое целое,  $g(\alpha) \neq 0$ . Если имеется такое целое число  $k \geq 0$ , что  $g(\alpha)$  не делится  $k$  раз на рассмат-

риваемый простой дивизор, то прямо из определения ясно, что должно существовать по крайней мере одно такое целое число  $\mu$ ,  $0 \leq \mu < k$ , что  $g(\alpha)$  делится точно  $\mu$  раз. Как мы уже видели, тогда  $g(\alpha) \Psi(\eta)^\mu / r^\mu$  уже не делится. Значит, для любого  $j \geq 0$  частное  $g(\alpha) \Psi(\eta)^{\mu+j} / r^\mu$  вовсе не делится и, следовательно,  $g(\alpha)$  не делится с кратностью  $\mu + j$  при  $j > 0$ . В частности,  $g(\alpha)$  не делится с кратностью  $t$ , когда  $t > k$ .

Для доказательства последнего утверждения предложения достаточно доказать, что имеется такое целое  $k$ , что  $g(\alpha)$  не делится  $k$  раз, поскольку тогда точная кратность  $\mu$ , с которой  $g(\alpha)$  делится, будет однозначно определена как наибольшее целое число  $\mu$ , такое, что  $g(\alpha)$  делится  $\mu$  раз. Для этого заметим, что если  $g(\alpha)$  делится  $k$  раз, то это же можно сказать и о  $Ng(\alpha)$ . Пусть  $Ng(\alpha) = r^n q$ , где  $n \geq 0$  и  $q$  не делится на  $r$ . Тогда  $Ng(\alpha)$  делится точно  $n$  раз и не может, следовательно, делиться  $k$  раз, когда  $k > n$ . Предложение доказано.

Второе определение, нужное для основной теоремы, — это определение единственного простого дивизора числа  $\lambda$ . Таким дивизором является делитель  $\alpha - 1$  числа  $\lambda$ .

**Определение.** *Простым дивизором* в арифметике круговых целых (для фиксированного простого  $\lambda > 2$ ) является либо (а) один из  $e$  простых дивизоров некоторого простого  $p \neq \lambda$ , определенных выше, либо (б) простой дивизор  $\alpha - 1$  числа  $\lambda$ . Простые дивизоры первого типа описываются заданием простого числа  $p \neq \lambda$  и целых  $u_1, u_2, \dots, u_e$ , как это делалось в предыдущем параграфе. Если заданы круговое целое  $g(\alpha) \neq 0$  и некоторый простой дивизор, то имеется *кратность*  $\mu \geq 0$ , с которой  $g(\alpha)$  делится на этот простой дивизор. Для простого дивизора первого типа эта кратность определяется как *точная* кратность, с которой  $g(\alpha)$  делится на этот простой дивизор в том смысле, как это было определено выше. Для единственного простого дивизора второго типа она определяется как число раз, которое  $\alpha - 1$  делит  $g(\alpha)$ .

**Предложение.** *Сравнимость по модулю  $\alpha - 1$  рефлексивна, симметрична, транзитивна и согласована со сложением и умножением. Кроме того,  $\alpha - 1$  — простое, т. е. из  $g_1(\alpha) g_2(\alpha) \equiv 0 \pmod{\alpha - 1}$  вытекает, что либо  $g_1(\alpha) \equiv 0$ , либо  $g_2(\alpha) \equiv 0 \pmod{\alpha - 1}$ . Целое число тогда и только тогда делится на  $\alpha - 1$ , когда оно делится на  $\lambda$ . Кратность, с которой  $g(\alpha) \neq 0$  делится на  $\alpha - 1$ , определена корректно, т. е. имеется такое  $\mu \geq 0$ , что  $(\alpha - 1)^\mu$  делит  $g(\alpha)$ , но  $(\alpha - 1)^{\mu+1}$  не делит его. Если  $\alpha - 1$  делит как  $g_1(\alpha)$ , так и  $g_2(\alpha)$  с кратностью по крайней мере  $\mu$ , то  $\alpha - 1$  делит  $g_1(\alpha) + g_2(\alpha)$  с кратностью по крайней мере  $\mu$ . Если  $\alpha - 1$  делит  $g_1(\alpha)$  с кратностью точно  $\mu$ , а  $g_2(\alpha)$  с кратностью точно  $\nu$ , то  $\alpha - 1$  делит  $g_1(\alpha) g_2(\alpha)$  с крат-*



ностью точно  $\mu + \nu$ . Наконец,  $\lambda$  тогда и только тогда делит  $g(\alpha)$ , когда  $\alpha - 1$  делит  $g(\alpha)$  с кратностью по крайней мере  $\lambda - 1$ .

*Доказательство.* Как мы видели в § 4.3,  $\alpha - 1$  тогда и только тогда делит  $g(\alpha)$ , когда  $g(1) \equiv 0 \pmod{\lambda}$ . Это показывает, что  $\alpha - 1$  — простое. Все утверждения, кроме последнего, элементарны. Последнее утверждение вытекает из того факта, что  $\lambda = (\alpha - 1)(\alpha^2 - 1) \dots (\alpha^{\lambda-1} - 1) = (\alpha - 1)^{\lambda-1} \cdot \text{единица}$ .

#### 4.11. Основная теорема

**Теорема.** Пусть  $\lambda$  — данное простое число, большее 2, и пусть  $g(\alpha)$  и  $h(\alpha)$  — два ненулевых круговых целых, построенных при помощи корня  $\alpha \neq 1$  из единицы степени  $\lambda$ . Тогда  $g(\alpha)$  в том и только в том случае делит  $h(\alpha)$ , когда каждый простой дивизор, делящий  $g(\alpha)$ , делит также и  $h(\alpha)$  с неменьшей кратностью.

*Доказательство.* Если  $g(\alpha)$  делит  $h(\alpha)$ , скажем  $h(\alpha) = q(\alpha)g(\alpha)$ , то, разумеется, каждый простой дивизор, делящий  $g(\alpha)$ , делит и  $h(\alpha)$  с неменьшей кратностью. Требуется доказать обратное утверждение. Сразу же заметим, что  $g(\alpha)$  тогда и только тогда делит  $h(\alpha)$ , когда  $Ng(\alpha) = g(\alpha)g(\alpha^2) \dots g(\alpha^{\lambda-1})$  делит  $Nh(\alpha) = h(\alpha)h(\alpha^2) \dots h(\alpha^{\lambda-1})$ . Если каждый простой дивизор, делящий  $g(\alpha)$ , делит также и  $h(\alpha)$  с неменьшей кратностью, то на основании правила, по которому комбинируются кратности при умножении, каждый простой дивизор, делящий целое число  $Ng(\alpha)$ , делит также и  $h(\alpha)h(\alpha^2) \dots h(\alpha^{\lambda-1})$  с неменьшей кратностью. Значит, достаточно доказать теорему в частном случае, когда  $g(\alpha)$  — целое число.

Пусть теперь  $g(\alpha)$  есть простое число  $p \neq \lambda$ ; тогда доказываемое утверждение означает, что если  $h(\alpha)$  делится на каждый из  $e$  простых дивизоров числа  $p$ , то  $h(\alpha)$  делится на  $p$ . Это было доказано в § 4.9. В случае  $g(\alpha) = \lambda$  утверждение состоит в том, что если  $(\alpha - 1)^{\lambda-1}$  делит  $h(\alpha)$ , то  $\lambda$  делит  $h(\alpha)$ . Это непосредственно видно из равенства  $\lambda = (\alpha - 1)^{\lambda-1} \cdot \text{единица}$ . Следовательно, достаточно доказать, что если теорема верна для деления на  $g_1(\alpha)$  и для деления на  $g_2(\alpha)$ , то она верна для деления на  $g_1(\alpha) \cdot g_2(\alpha)$ . Но это совсем легко. Если каждый простой дивизор, делящий  $g_1(\alpha)g_2(\alpha)$ , делит также и  $h(\alpha)$  с неменьшей кратностью и если теорема верна для деления на  $g_1(\alpha)$ , то  $g_1(\alpha)$  делит  $h(\alpha)$ , т. е.  $h(\alpha) = g_1(\alpha)h_1(\alpha)$ . На основании правила, по которому комбинируются кратности, отсюда следует, что каждый простой дивизор, делящий  $g_2(\alpha)$ , делит также и  $h_1(\alpha)$  с неменьшей кратностью. Если теорема верна для деления на  $g_2(\alpha)$ , то отсюда следует, что  $h_1(\alpha) = g_2(\alpha)h_2(\alpha)$  для некоторого  $h_2(\alpha)$ .



Следовательно,  $h(\alpha) = g_1(\alpha) g_2(\alpha) h_2(\alpha)$  и  $h(\alpha)$  делится на  $g_1(\alpha) g_2(\alpha)$ , что и требовалось показать. Это завершает доказательство основной теоремы.

Эта теорема и «спасает» свойство единственности разложения на простые в следующем смысле.

**Следствие.** Если два круговых целых  $g(\alpha)$  и  $h(\alpha)$  делятся в точности на одни и те же простые дивизоры с точно совпадающими кратностями, то они отличаются только на сомножитель, являющийся единицей, т. е.  $g(\alpha) = \text{единица} \cdot h(\alpha)$ .

**Доказательство.** По основной теореме,  $g(\alpha)$  делит  $h(\alpha)$  и  $h(\alpha)$  делит  $g(\alpha)$ . Значит,  $h(\alpha)/g(\alpha)$  и  $g(\alpha)/h(\alpha)$  — круговые целые. Так как их произведение равно 1, то они оба должны быть единицами.

Конечно, кое-что теряется. Хотя «разложение» кругового целого определяет это круговое целое с точностью до сомножителя, являющегося единицей, здесь уже неверно, в отличие от случая обычных целых чисел, что это «разложение» может быть предписано произвольно. Например, при  $\lambda = 23$  невозможно найти круговое целое, которое делилось бы один раз на один простой дивизор числа 47, но не делилось бы ни на какой другой простой дивизор. Возникает очень естественный и очень важный вопрос: *какие* «разложения» действительно возможны? Этот вопрос совершенно естественно приводит, как будет показано в гл. 5, к понятию эквивалентности и к *группе классов дивизоров* — конечной группе, структура которой дает средства описания тонких фактов из арифметики круговых целых. Заключительные параграфы этой главы посвящены развитию символики и терминологии для изложения теории Куммера в удобной форме.

### Упражнения

1. Докажите, что если  $p \neq \lambda$  — простое число с показателем  $f$  по модулю  $\lambda$  и  $g(\alpha)$  — круговое целое с нормой  $p^f$ , то  $g(\alpha)$  делится на один простой дивизор числа  $p$  и не делится на другие. Выведите отсюда, что  $g(\alpha)$  простое и что оно тогда и только тогда  $\mu$  раз делит  $h(\alpha)$ , когда  $h(\alpha)$  делится с кратностью  $\mu$  на тот простой дивизор числа  $p$ , который делит  $g(\alpha)$ .

2. Докажите, что если  $Ng(\alpha) = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}$  — обычное разложение на простые сомножители целого числа  $Ng(\alpha)$ , то для каждого  $i$  число  $g(\alpha)$  делится точно на  $\mu_i/f_i$  простых дивизоров числа  $p_i$  (с учетом кратностей), где  $f_i$  — показатель числа  $p_i$  по модулю  $\lambda$ , когда  $p_i \neq \lambda$ , и  $f_i = 1$ , когда  $p_i = \lambda$ .

## 4.12. Дивизоры

Как обычно, пусть  $\lambda$  — фиксированное простое число, большее 2, и пусть выражение «круговое целое» означает круговое целое, построенное при помощи корня  $\alpha \neq 1$  из единицы степе-

ни  $\lambda$ . *Дивизором ненулевого кругового целого  $g(\alpha)$*  назовем список всех простых дивизоров, делящих  $g(\alpha)$ , с учетом кратностей, т. е. список простых дивизоров, который состоит из всех простых дивизоров, делящих  $g(\alpha)$ , причем каждый из них встречается в списке столько раз, какова кратность, с которой он делит  $g(\alpha)$ . *Дивизором* называется любой конечный список простых дивизоров. Данный простой дивизор может встречаться в дивизоре более одного раза, т. е. с некоторой кратностью. *Пустой* список тоже рассматривается как дивизор; это дивизор кругового целого 1. *Произведение* двух дивизоров есть объединение двух списков, т. е. список, содержащий все простые дивизоры с учетом кратностей, которые находятся в двух данных списках. С этой точки зрения произвольный дивизор можно рассматривать как произведение простых дивизоров. Говорят, что один дивизор *делится* на другой дивизор, если первый может быть записан в виде произведения второго на некоторый третий дивизор. Говорят, что круговое целое делится на дивизор, если его дивизор делится на этот дивизор, и, аналогично, говорят, что дивизор делится на круговое целое, если он делится на дивизор этого кругового целого. Делитель кругового целого — это любой дивизор, который его делит, или, когда это ясно из контекста, любое круговое целое, которое его делит.

В соответствии с этим определением основная теорема утверждает, что для двух ненулевых круговых целых  $g(\alpha)$ ,  $h(\alpha)$  одно из них  $g(\alpha)$  тогда и только тогда делит второе  $h(\alpha)$ , когда дивизор первого делит дивизор второго. Заметим также, что правило комбинирования кратностей при умножении можно сформулировать так: дивизор произведения равен произведению дивизоров. Так как 0 делится на любое ненулевое круговое целое  $g(\alpha)$ , то иногда удобно рассматривать 0 как дивизор, содержащий каждый простой дивизор в бесконечном числе экземпляров. Теорема о том, что разложение на простые дивизоры единственно, является утверждением о том, что два круговых целых  $g(\alpha)$ ,  $h(\alpha)$ , имеющие один и тот же дивизор, различаются на сомножитель, который есть единица,  $g(\alpha) = \text{единица} \cdot h(\alpha)$ . Нарушение единственности разложения на *реально существующие* простые сомножители, когда оно встречается, отражает тот факт, что заданный дивизор не обязан быть дивизором кругового целого. Например, при  $\lambda = 23$  дивизор числа  $47 \cdot 139$  есть произведение 22 простых дивизоров числа 47 и 22 простых дивизоров числа 139. Ни один из этих 44 простых дивизоров не является дивизором какого-либо кругового целого. Два разложения числа  $47 \cdot 139$ , которые были описаны в конце § 4.4, показывают, что есть два совершенно различных способа перегруппировки этих 44 дивизоров в 22 пары так, что каждая пара есть дивизор некоторого реального кругового целого.

Так как основным понятием всей теории является понятие простого дивизора, удобно иметь более сжатое обозначение простых дивизоров, чем фраза «простой дивизор числа  $p$ , соответствующий набору целых чисел  $u_1, u_2, \dots, u_e$ , обладающему свойством, описанным в предложении из § 4.9». (Один исключительный простой дивизор можно, конечно, обозначать просто через  $\alpha - 1$ .) Куммер не ввел более короткого обозначения, и это упущение, возможно, замедлило принятие его теории. Однако он пользовался описанием простых дивизоров в терминах определяемых далее круговых целых  $\psi(\eta)$ , и это позволило ему обращаться с простыми дивизорами без заметных неудобств и затруднений.

**Теорема.** *Для любого данного простого дивизора числа  $p \neq \lambda$  имеется круговое целое  $\psi(\eta)$ , образованное периодами длины  $f$  (показатель числа  $p$  по модулю  $\lambda$ ), которое делится точно один раз на этот простой дивизор числа  $p$  и не делится на остальные  $e - 1$  простых дивизоров числа  $p$ . Следовательно, круговое целое  $g(\alpha)$  тогда и только тогда делится с кратностью  $\mu$  на данный простой дивизор числа  $p$ , когда  $g(\alpha) [\sigma\psi(\eta)]^\mu [\sigma^2\psi(\eta)]^\mu \dots [\sigma^{e-1}\psi(\eta)]^\mu$  делится на  $p^\mu$ .*

**Доказательство.** Пусть  $\Psi(\eta)$  соответствует в прежнем смысле данному простому дивизору числа  $p$ , т.е. пусть  $u_1, u_2, \dots, u_e$  — такие целые числа, что  $u_i - \eta_i$  делятся на данный простой дивизор, и пусть  $\Psi(\eta)$  — произведение  $e p - e$  сомножителей  $j - \eta_i$ , где  $j \neq u_i$ . Тогда  $\Psi(\eta)$  делится на все  $e$  простых дивизоров числа  $p$ , кроме данного. Далее,  $\varphi(\eta) = \sigma\Psi(\eta) + \sigma^2\Psi(\eta) + \dots + \sigma^{e-1}\Psi(\eta)$  делится на данный простой дивизор числа  $p$  (каждое слагаемое суммы делится на него), но не делится на остальные  $e - 1$  простых дивизоров числа  $p$  (поскольку для каждого из них все слагаемые, кроме одного, делятся на него, а это одно не делится). Если  $\varphi(\eta)$  делится с кратностью точно 1 на данный простой дивизор числа  $p$ , то элемент  $\psi(\eta) = \varphi(\eta)$  обладает требуемым свойством. Если  $\varphi(\eta)$  делится с кратностью, большей 1, то полагаем  $\psi(\eta) = \varphi(\eta) + p$ . Тогда элемент  $\psi(\eta)$  не делится на  $e - 1$  простых дивизоров, отличных от данного (поскольку если бы это было не так, то делился бы и  $\varphi(\eta) = \psi(\eta) - p$ ), делится на данный простой дивизор числа  $p$  (поскольку  $\varphi(\eta)$  делится) и не делится на данный простой дивизор с кратностью, большей 1 (поскольку иначе это было бы так и для  $p = \psi(\eta) - \varphi(\eta)$ ). Это завершает конструкцию элемента  $\psi(\eta)$ . Второе утверждение теоремы является непосредственным следствием основной теоремы.

**Теорема.** *Круговые целые, которые назывались «простыми» в § 4.7, действительно простые. Вообще, если  $p \neq \lambda$  — простое*

число, показатель которого по модулю  $\lambda$  равен  $f$ , и если  $g(\alpha)$  — круговое целое, норма которого равна  $p^f$ , то  $g(\alpha)$  простое. [Если  $g(\alpha) = g(\eta)$  образовано периодами длины  $f$ , то условие  $Ng(\alpha) = p^f$  можно также сформулировать в виде  $g(\eta) \cdot \sigma g(\eta) \cdot \dots \cdot \sigma^{e-1} g(\eta) = \pm p$ .]

*Доказательство.* Пусть  $v_1, v_2, \dots, v_e$  — точные кратности, с которыми простые дивизоры числа  $p$  делят  $g(\alpha)$ . Тогда  $\sigma g(\alpha)$  делится на эти простые дивизоры с точными кратностями  $v_2, v_3, \dots, v_e, v_1, \sigma^2 g(\alpha)$  — с точными кратностями  $v_3, v_4, \dots, v_2$ , и т. д. Следовательно, каждый простой дивизор числа  $p$  делит  $Ng(\alpha)$  с точной кратностью  $(v_1 + v_2 + \dots + v_e)f$ . Если  $Ng(\alpha) = p^f$ , то одно из  $v_i$  должно быть 1, а остальные 0. Тогда, по основной теореме, делимость на  $g(\alpha)$  совпадает с делимостью на простой дивизор, а отсюда следует, что  $g(\alpha)$  простое.

*Обозначения.* Пусть задан простой дивизор числа  $p$ , и пусть  $\psi(\eta)$  — круговое целое, о котором говорится в теореме, т. е. круговое целое, образованное периодами длины  $f$  (показатель числа  $p$  по модулю  $\lambda$ ), которое делится точно один раз на рассматриваемый простой дивизор числа  $p$  и не делится ни на один из остальных  $e - 1$  дивизоров числа  $p$ . Тогда данный простой дивизор будем обозначать через  $(p, \psi(\eta))$ . Так как этот дивизор делит  $p$  и  $\psi(\eta)$ , причем оба с кратностью точно 1, а ни один другой простой дивизор их оба не делит, то  $(p, \psi(\eta))$  есть *наибольший общий делитель* числа  $p$  и кругового целого  $\psi(\eta)$ . Таким образом, обозначение  $(p, \psi(\eta))$  согласуется с общепринятым обозначением наибольшего общего делителя двух чисел. Если можно найти такое  $\psi(\eta)$  с дополнительным свойством, чтобы его дивизор *совпадал* с рассматриваемым простым дивизором числа  $p$ , то этот простой дивизор также будет обозначаться через  $(\psi(\eta))$ . Единственный простой дивизор числа  $\lambda$  будет обозначаться  $(\alpha - 1)$  (в противоположность обозначению  $\alpha - 1$  без скобок, применяемому для кругового целого, дивизором которого является  $(\alpha - 1)$ ). Дивизоры будут, как правило, обозначаться заглавными латинскими буквами  $A, B, C, \dots$ , а их произведение, как обычно, — простым приписыванием букв. Так,  $AB$  обозначает произведение дивизоров  $A$  и  $B$ . Кроме того,  $A^n$ , где  $n$  — положительное целое число, будет обозначать произведение  $A$  с самим собой  $n$  раз. Произвольный дивизор  $A$  может быть записан в виде

$$(p_1, \psi_1)^{\mu_1} (p_2, \psi_2)^{\mu_2} \dots (p_m, \psi_m)^{\mu_m},$$

где (при каждом  $i = 1, 2, \dots, m$ )  $p_i$  — простое целое число,  $\mu_i$  — положительное целое число, а  $\psi_i$  — круговое целое, образованное периодами длины  $f_i$  (где  $f_i$  — показатель числа  $p_i$  по модулю  $\lambda$ , или если  $p_i = \lambda$ , то  $f_i = 1$ ), дивизор которого содержит

один простой дивизор числа  $p_i$  с кратностью точно 1 и не содержит никаких других простых дивизоров числа  $p_i$ . Если дивизор элемента  $\psi_i$  равен простому дивизору числа  $p_i$ , то  $p_i$  можно опустить и записать дивизор  $(p_i, \psi_i)^{u_i}$  как  $(\psi_i)^{u_i}$ . Пустой дивизор обозначается через  $I$ , а степень дивизора  $A$  с показателем 0 определяется равенством  $A^0 = I$ .

## Упражнения

1. Куммер утверждает ([K8], стр. 333), что если набор целых чисел  $u_1, u_2, \dots, u_e$  содержит одно число  $u_j$  с кратностью 1, то  $u_j - \eta_0$  делится на один из  $e$  простых дивизоров числа  $p$  с кратностью точно 1 и не делится на остальные  $e - 1$  дивизоров. Это утверждение содержит небольшую ошибку. Докажите, что  $u_j + kp - \eta_0$  обладает указанным свойством точно для  $p - 1$  из возможных  $p$  значений числа  $k$  по модулю  $p$ . Докажите более общее утверждение: если  $\varphi(\eta)$  делится точно на один простой дивизор числа  $p$ , то тем же свойством обладает  $\varphi(\eta) + kp$  для всех целых  $k$ , и кратность, с которой этот простой дивизор его делит, равна 1 для  $p - 1$  из возможных по модулю  $p$  значений числа  $k$  и больше 1 для одного оставшегося значения.

2. В случае  $\lambda = 31$  напишите простые дивизоры числа 2 в виде  $(2, \psi)$ .

3. Каковы в обозначениях, введенных в этом параграфе, простые дивизоры числа 47 в случае  $\lambda = 23$ ?

4. Используя упр. 1, дайте необходимое и достаточное условие того, чтобы «разложение» числа  $p \neq \lambda$  имело вид

$$(p) = (p, \eta_0 - u) (p, \eta_1 - u) \dots (p, \eta_{e-1} - u)$$

для некоторого целого  $u$ .

5. Докажите, что для любого данного дивизора  $A$  число не сравнимых по модулю  $A$  круговых целых конечно. [Найдите такое целое число  $n$ , чтобы из сравнимости по модулю  $A$  вытекала сравнимость по модулю  $n$ .]

6. Пусть  $\psi(\eta)$  — круговое целое, образованное периодами длины  $f$ , и пусть  $p$  — простое число, показатель которого по модулю  $\lambda$  равен  $f$ . Покажите, что  $\psi(\eta)$  тогда и только тогда делится на единственный простой дивизор числа  $p$ , причем с кратностью 1, когда  $N\psi(\eta)$  делится на  $p^f$ , но не делится на  $p^{f+1}$ .

## 4.13. Терминология

Куммер называл круговые целые «комплексными числами» или, когда он выражался подробнее, «комплексными числами, построенными из комплексного корня степени  $\lambda$  из единицы». Дивизоры он называл «идеальными комплексными числами». Этот последний оборот речи был весьма неудачным по нескольким причинам. Во-первых, хотя «комплексное число» (круговое целое) действительно определяет «идеальное комплексное число» (дивизор), но много различных комплексных чисел определяют таким способом одно и то же идеальное комплексное число, поскольку круговые целые, которые отличаются на множитель, являющийся единицей, имеют один и тот же дивизор. Таким образом «идеальное комплексное число» не является каким-то обобщением «комплекс-



ного числа», на что намекает терминология Куммера. Кроме того, нет разумного способа определить сложение дивизоров, а название «числа» для объектов, которые нельзя складывать, безусловно, вводит в заблуждение. Другим недостатком терминологии Куммера является семантическая проблема, возникающая из-за того, что у Куммера идеальное комплексное число *может* оказаться реальным комплексным числом, поэтому может возникнуть необходимость отличать «реальные» идеальные комплексные числа от «идеальных» идеальных комплексных чисел. Более того, хотя Куммер, когда он вводил этот термин, имел в виду некоторые красивые и ясные аналогии (см., в частности, первую страницу его сообщения [К7] и заключительные замечания в § 10 его главной статьи [К8] по теории идеального разложения), эти аналогии не стали для его последователей ни привлекательными, ни полезными. Наконец, термин «идеальное комплексное число» имеет еще тот большой психологический вред, что почти неизбежно ведет к вопросу: «Что такое идеальное комплексное число?» Этот вопрос открывает тот же ящик Пандоры метафизических измышлений, как и вопросы: «Что такое натуральное число?» или «Что такое вещественное число?», — и дать на него окончательный ответ ничуть не легче, чем решить эти старинные загадки. (Конечно, рассуждая логически, Куммеру не было нужды заниматься этим вопросом, и он не занимался. Он подробно описал, как следует представлять идеальные комплексные числа и как выполнять над ними вычисления, что, по существу, и является ответом, который дает математик-практик на вопрос «что такое число?»; см. [Е1], в частности «The Parable of the Logician and the Carpenter».) По всем этим причинам современная терминология на языке дивизоров предпочтительнее терминологии Куммера на языке идеальных комплексных чисел.

Термин «дивизор» отвечает наиболее общей ситуации, когда дивизоры используются. Понятие «простого дивизора» появилось в § 4.9, когда понадобилось выяснить смысл высказывания о том, что данное круговое целое *делится* на такой простой дивизор. В более общей форме, для такого простого дивизора  $A$  было определено утверждение:  $g_1(\alpha) \equiv g_2(\alpha) \pmod{A}$ . Для любого дивизора  $A$ , простого или нет, можно определить сравнение  $g_1(\alpha) \equiv g_2(\alpha) \pmod{A}$ , которое означает, что  $g_1(\alpha) - g_2(\alpha)$  делится на  $A$  в том смысле, как определено в предыдущем параграфе. Значение дивизоров  $A$  проявляется главным образом в утверждениях  $g_1(\alpha) \equiv g_2(\alpha) \pmod{A}$ . С этой точки зрения следующая теорема позволяет сделать важный вывод, что для определения дивизора  $A$  достаточно знать отношение  $g_1(\alpha) \equiv g_2(\alpha) \pmod{A}$ .

**Теорема.** Пусть  $A$  и  $B$  — дивизоры. Если каждое круговое целое, делящееся на  $A$ , делится также и на  $B$ , то  $A$  делится на  $B$ .



**Следствие.** Если  $A$  и  $B$  — дивизоры и отношение  $g_1(\alpha) \equiv g_2(\alpha) \pmod{A}$  равносильно отношению  $g_1(\alpha) \equiv g_2(\alpha) \pmod{B}$  (т. е. одно отношение выполняется тогда и только тогда, когда выполняется другое), то  $A = B$ .

**Доказательство.** Следствие вытекает из замечания, что если  $A$  делит  $B$  и  $B$  делит  $A$ , то  $A = B$ . Пусть  $p_1, p_2, \dots, p_n$  — простые целые числа, которые делятся на простые дивизоры, делящие  $A$  (другими словами, числа  $p_i$  являются простыми делителями нормы дивизора  $A$  — см. следующий параграф), и пусть  $A = A_1 A_2 \dots A_n$  — разложение дивизора  $A$  в произведение таких дивизоров  $A_i$ , что  $A_i$  содержит все простые дивизоры из  $A$ , которые делят  $p_i$ . Так как достаточно высокая степень числа  $p_1 p_2 \dots p_n$  делится на  $A$ , то, по предположению, она должна делиться и на  $B$ . Отсюда вытекает, что каждый простой дивизор из  $B$  делит одно из чисел  $p_i$ , и, значит,  $B$  может быть разложено в произведение  $B = B_1 B_2 \dots B_n$ , в котором  $B_i$  содержит все простые дивизоры из  $B$ , делящие  $p_i$ . (Некоторые из  $B_i$  могут быть равны  $I$ .) Так как порядок чисел  $p_i$  произволен, то достаточно доказать, что  $B_1$  делит  $A_1$ . Если  $p_1 = \lambda$ , то  $A_1 = (\alpha - 1)^\mu$  при некотором  $\mu$ . Тогда круговое целое  $(\alpha - 1)^\mu (p_2 p_3 \dots p_n)^\nu$  делится на  $A$  при всех достаточно больших  $\nu$ . Значит, оно также делится на  $B$  при больших  $\nu$ , и поскольку  $B_1$  не делит  $(p_2 p_3 \dots p_n)^\nu$ , то  $B_1$  делит круговое целое  $(\alpha - 1)^\mu$ . Следовательно,  $B_1$  делит дивизор элемента  $(\alpha - 1)^\mu$ , который есть  $A_1$ . Если  $p_1 \neq \lambda$ , то пусть  $f$  — показатель числа  $p_1$  по модулю  $\lambda$ , и пусть  $\psi$  — круговое целое, образованное периодами длины  $f$ , делящееся на один из  $e = (\lambda - 1)/f$  простых дивизоров числа  $p_1$  с кратностью 1 и не делящееся ни на один из остальных  $e - 1$  простых дивизоров. Тогда можно образовать произведение сопряженных элемента  $\psi$ , назовем его  $x$ , обладающее таким свойством: дивизор элемента  $x$  есть дивизор  $A_1$ , умноженный на простые дивизоры, не делящие  $p_1$ . Теперь число  $x (p_2 p_3 \dots p_n)^\nu$  делится на  $A$  при большом  $\nu$ ; значит, оно делится на  $B_1$ . Так как  $B_1$  не делит  $(p_2 p_3 \dots p_n)^\nu$ , то отсюда вытекает, что  $B_1$  делит дивизор элемента  $x$ . Так как дивизор элемента  $x$  есть  $A_1$ , умноженный на дивизор, не содержащий ни одного простого дивизора числа  $p_1$  (и тем более ни одного простого дивизора из  $B_1$ ), то  $B_1$  делит  $A_1$ , что и требовалось доказать.

Рихард Дедекин (1831—1916), который провел важную работу по обобщению теории Куммера, не сохранил куммеровской терминологии. Он очень глубоко вник в философский вопрос: «Что такое число?» и по поводу куммеровых «идеальных комплексных чисел» дал ответ, который оказал глубокое влияние на терминологию всей математики. Дедекин воспользовался доказанным выше утверждением о том, что дивизор определяется множеством всех тех круговых целых, которые он делит, и *идентифицировал*

идеальное комплексное число с множеством всех делящихся на него объектов. Это множество он назвал *идеалом* — такую причудливую трансформацию претерпела терминология Куммера. Затем Дедекиннд показал, что среди всех подмножеств круговых целых «идеалы» характеризуются двумя свойствами:

(i) Сумма любых двух круговых целых из данного идеала также лежит в этом идеале.

(ii) Произведение кругового целого из данного идеала на любое круговое целое также лежит в этом идеале.

То, что идеалы обладают этими свойствами, очевидно: из  $g_1(\alpha) \equiv 0$ ,  $g_2(\alpha) \equiv 0 \pmod{A}$  вытекает  $g_1(\alpha) + g_2(\alpha) \equiv 0 \pmod{A}$  и  $g_1(\alpha) \varphi(\alpha) \equiv 0 \pmod{A}$  для всех  $\varphi(\alpha)$ . Однако Дедекиннд доказал и обратное, что *каждое* подмножество круговых целых с этими свойствами есть идеал, т. е. является множеством всех круговых целых, делящихся на  $A$ , где  $A$  — некоторый дивизор. [Для того чтобы это было верно в полной общности, мы должны определить дивизор нуля как дивизор, обладающий тем свойством, что на него делится *только* нуль. См. упр. 3.] После этого можно охарактеризовать простые дивизоры без какого бы то ни было явного нахождения их, а следовательно, дать абстрактное описание теории, не занимаясь фактическим построением простых дивизоров. Этот подход особенно полезен при изучении обобщения теории Куммера на другие типы алгебраических целых, отличных от круговых целых; выполнение такого обобщения было одним из главных достижений Дедекиннда.

Терминология Дедекиннда и, в частности, понятие «идеала» играют очень важную роль в современной абстрактной алгебре. Однако в последующих разделах этой книги, помимо идеалов, будет использоваться более конструктивное и более связанное с вычислениями понятие «дивизора». Иными словами, мы принимаем более конкретные и явные формулировки Куммера, хотя и не принимаем его терминологию.

## Упражнения

1. Какое третье условие нужно добавить к приведенным в тексте свойствам (i) и (ii), чтобы охарактеризовать *простые* идеалы, т. е. идеалы, которые возникают из простых дивизоров?

2. Пусть  $\mathcal{J}$  — произвольное подмножество круговых целых, обладающее свойствами (i) и (ii). Покажите, что имеется такой конечный набор  $g_1(\alpha), g_2(\alpha), \dots, g_n(\alpha)$  круговых целых, что  $\mathcal{J}$  состоит из всех круговых целых, которые можно записать в виде  $b_1(\alpha)g_1(\alpha) + b_2(\alpha)g_2(\alpha) + \dots + b_n(\alpha)g_n(\alpha)$  при некоторых круговых целых  $b_1(\alpha), b_2(\alpha), \dots, b_n(\alpha)$ . [Если  $\mathcal{J}$  состоит из одного 0, то положите  $n = 1$  и  $g_1(\alpha) = 0$ . В противном случае в  $\mathcal{J}$  выберите  $g_1(\alpha) \neq 0$ . Покажите, что имеется лишь конечное число не сравнимых по модулю  $g_1(\alpha)$  элементов. Из каждого класса по модулю  $g_1(\alpha)$ , содержащего элемент из  $\mathcal{J}$ , выберите по одному такому элементу и поместите его среди  $g_2(\alpha), g_3(\alpha), \dots, g_n(\alpha)$ . Построенные таким способом  $g_i$  имеют требуемые свойства.]

3. Используйте упр. 2 для нахождения того, каким должен быть дивизор, соответствующий идеалу  $\mathcal{J}$ . [Если  $\mathcal{J} = \{0\}$ , то никакой дивизор не подойдет, кроме «дивизора», содержащего *все* простые дивизоры с *бесконечными* кратностями. Оправданием такого определения дивизора нуля служит то, что 0 делится на что угодно и не делит ничего, кроме самого себя.] Доказательство того, что каждое подмножество  $\mathcal{J}$ , обладающее свойствами (i), (ii), есть множество объектов, делящихся на некоторый дивизор, изучается в упр. 3 к § 4.14.

#### 4.14. Сопряжения и норма дивизора

Точно так же как сопряжения  $\alpha \mapsto \alpha^j$  действуют на круговые целые, они естественным образом действуют на *дивизоры*. Именно, пусть  $\sigma$  — сопряжение  $\alpha \mapsto \alpha^\gamma$ , где  $\gamma$  — примитивный корень по модулю  $\lambda$ , так что сопряжения можно записывать в виде степеней этого сопряжения  $\sigma$  без использования двойных показателей. Для того чтобы описать действие на дивизоры сопряжения общего вида  $\sigma^i$ , достаточно описать действие на них самого  $\sigma$ , поскольку  $\sigma^i$  есть композиция  $\sigma$  самого с собой  $i$  раз. А это можно описать, например, следующим способом.

Так как, по определению,  $\sigma(AB)$  равно  $\sigma(A) \cdot \sigma(B)$ , то достаточно описать действие сопряжения  $\sigma$  на *простые* дивизоры. Для этого легче всего записать простой дивизор в виде  $(p, \psi(\eta))$ , как в § 4.12, и определить  $\sigma(p, \psi(\eta))$  как  $(p, \sigma\psi(\eta))$ . (Особый дивизор  $(\alpha - 1)$  равен всем своим сопряженным, поскольку  $\alpha^\gamma - 1$  имеет тот же дивизор, что и  $\alpha - 1$ .) Это и определяет действие сопряжения  $\sigma$  на дивизоры. Легко проверить, что это действие обладает следующим естественным свойством.

**Предложение 1.** Пусть  $\sigma$  — сопряжение круговых целых,  $g_1(\alpha)$ ,  $g_2(\alpha)$  — круговые целые,  $A$  — некоторый дивизор. Тогда сравнение  $g_1(\alpha) \equiv g_2(\alpha) \pmod{\sigma^i A}$  равносильно сравнению  $\sigma^{-i} g_1(\alpha) \equiv \sigma^{-i} g_2(\alpha) \pmod{A}$ .

*Доказательство.* См. упр. 1.

Предложение 1 описывает сравнимость по модулю  $\sigma^i A$  в терминах тех понятий, которые уже были определены в предыдущих параграфах, и, следовательно, поскольку дивизор определяется посредством соответствующего отношения сравнимости, предложение дает еще один путь *определения* сопряжения  $\sigma^i A$ .

Точно так же как норма кругового целого  $g(\alpha)$  определена как произведение  $g(\alpha) \cdot \sigma g(\alpha) \cdot \sigma^2 g(\alpha) \dots \sigma^{\lambda-2} g(\alpha)$ , норму дивизора  $A$  можно определить как произведение дивизоров  $A \cdot \sigma A \cdot \sigma^2 A \dots \sigma^{\lambda-2} A$ . Норма кругового целого есть такое круговое целое, которое (поскольку оно инвариантно относительно  $\sigma$ ) оказывается в действительности обычным целым числом, причем, как мы видели в § 4.2, это целое число неотрицательно. Норма дивизора есть *дивизор*. Однако, как показывает следующее предложе-

ние, его естественным образом можно рассматривать как положительное целое число

**Предложение 2.** *Если  $A$  — любой дивизор, то имеется положительное целое число, дивизор которого равен норме дивизора  $A$ .*

*Доказательство.* См. упр. 2.

Норма дивизора  $A$  будет обозначаться через  $N(A)$  или  $NA$ . По своему определению она есть дивизор, но в некоторых ситуациях, в частности в гл. 6, удобно рассматривать ее как положительное целое число, дивизором которого она является. Это положительное целое число можно также описать следующим простым способом.

**Теорема.** *Когда  $N(A)$  рассматривается как положительное целое число, она равна максимальному количеству не сравнимых по модулю  $A$  круговых целых. Иными словами, можно найти систему из  $N(A)$  круговых целых, обладающую тем свойством, что каждое круговое целое сравнимо по модулю  $A$  с одним и только одним элементом из этой системы.*

*Доказательство.* Если  $A$  — простой дивизор, то его норма есть  $p^f$ , где  $p$  — делящееся на него простое целое число, а  $f$  — показатель числа  $p$  по модулю  $\lambda$ ; тот факт, что эта норма равна также числу не сравнимых по модулю  $\lambda$  элементов, доказан в теореме 1 из § 4.9. (Если  $A$  — исключительный дивизор  $(1 - \alpha)$ , то каждое круговое целое сравнимо с одним и только одним из  $\lambda$  целых чисел  $0, 1, 2, \dots, \lambda - 1$ .)

Теперь рассмотрим случай, когда  $A$  является степенью простого дивизора  $P$ , т. е.  $A = P^n$ . Пусть  $\psi$  — круговое целое, которое делится на  $P$  с кратностью точно 1 и не делится ни на один из дивизоров, сопряженных дивизору  $P$ .

Далее будет показано, что каждое круговое целое сравнимо по модулю  $P^n$  с одним из элементов вида  $a_0 + a_1\psi + a_2\psi^2 + \dots + a_{n-1}\psi^{n-1}$  и что два круговых целых этого вида тогда и только тогда сравнимы по модулю  $P^n$ , когда коэффициенты  $a_0, a_1, \dots, a_{n-1}$  одинаковы по модулю  $P$ ; тем самым будет доказано, что число классов по модулю  $P^n$  равно числу способов выбора по модулю  $P$  коэффициентов  $a_0, a_1, \dots, a_{n-1}$ , которое есть  $N(P)^n = N(P^n)$ , что и требуется показать. При  $n = 1$  это очевидно. Предположим, что это доказано для  $n - 1$ . Тогда для данного кругового целого  $x$  имеются круговые целые  $a_0, a_1, \dots, a_{n-2}$ , для которых  $x \equiv a_0 + a_1\psi + \dots + a_{n-2}\psi^{n-2} \pmod{P^{n-1}}$  и коэффициенты  $a_0, a_1, \dots, a_{n-2}$  однозначно определены по модулю  $P$ . Пусть  $y = x - a_0 - a_1\psi - \dots - a_{n-2}\psi^{n-2}$ . Тогда  $y \equiv 0 \pmod{P^{n-1}}$ .

Сейчас нужно показать, что  $y \equiv a\psi^{n-1} \pmod{P^n}$  для некоторого  $a$  и что  $a$  однозначно определено по модулю  $P$ . Пусть  $\Psi$  обозначает произведение  $e - 1$  различных сопряженных элемента  $\psi$ , так что  $\psi\Psi = rk$ , где  $k$  — целое число, взаимно простое с  $p$ . Тогда требуемое сравнение  $y \equiv a\psi^{n-1} \pmod{P^n}$  равносильно сравнению  $y\Psi^{n-1} \equiv ar^{n-1}k^{n-1} \pmod{P^n}$ , которое в свою очередь равносильно сравнению  $y\Psi^{n-1}m^{n-1} \equiv ar^{n-1} \pmod{P^n}$ , где  $m$  — такое целое число, что  $mk \equiv 1 \pmod{p}$ . Так как  $y \equiv 0 \pmod{P^{n-1}}$  по предположению, то  $y\Psi^{n-1}m^{n-1}$  делится на  $p^{n-1}$ , и требуемое сравнение равносильно утверждению о том, что частное сравнимо по модулю  $P$  с  $a$ , из чего вытекает, как и требуется, что имеется одно и только одно по модулю  $P$  такое  $a$ . Это завершает доказательство в случае  $A = P^n$ . Общий случай теперь легко вытекает из обобщенной китайской теоремы об остатках.

**Китайская теорема об остатках.** Пусть  $A$  и  $B$  — взаимно простые дивизоры, и пусть  $a$  и  $b$  — круговые целые. Тогда сравнения  $x \equiv a \pmod{A}$  и  $x \equiv b \pmod{B}$  имеют решение  $x$ .

При помощи этой теоремы доказательство предыдущей теоремы можно завершить следующим образом. Число не сравнимых по модулю  $AB$  элементов не превосходит произведения числа элементов, не сравнимых по модулю  $A$ , на число элементов, не сравнимых по модулю  $B$ , поскольку из  $x \equiv x' \pmod{A}$  и  $x \equiv x' \pmod{B}$  вытекает  $x \equiv x' \pmod{AB}$  ( $A$  и  $B$  оба делят  $x - x'$  и взаимно просты, поэтому  $AB$  делит  $x - x'$ ), т. е. класс элемента  $x$  по модулю  $AB$  определен его классом по модулю  $A$  и его классом по модулю  $B$ . Китайская теорема об остатках показывает, что встречаются все возможные комбинации классов по модулю  $A$  и по модулю  $B$ , так что число классов по модулю  $AB$  равно произведению числа классов по модулю  $A$  на число классов по модулю  $B$ . По индукции, если  $A, B, C, \dots, D$  — попарно взаимно простые дивизоры, то число классов по модулю  $ABC \dots D$  равно произведению числа классов по модулю  $A$  на число классов по модулю  $B$ , на число классов по модулю  $C, \dots$ , на число классов по модулю  $D$ . Если  $A, B, C, \dots, D$  являются степенями простых дивизоров, то, как показано выше, это число равно  $N(A)N(B)N(C) \dots N(D) = N(ABC \dots D)$ . Так как дивизор может быть записан в виде  $ABC \dots D$ , где  $A, B, C, \dots, D$  — попарно взаимно простые степени простых дивизоров, то из этого следует, что число классов по модулю любого дивизора есть норма этого дивизора, что и требовалось показать.

**Доказательство китайской теоремы об остатках.** Из теоремы следует, что если  $A$  и  $B$  — взаимно простые дивизоры, то имеется круговое целое  $g$ , удовлетворяющее сравнениям  $g \equiv 1 \pmod{A}$  и  $g \equiv 0 \pmod{B}$ . Обратно, если известно, что это



утверждение верно, то, по симметрии, имеется также такое круговое целое  $h$ , что  $h \equiv 0 \pmod{A}$  и  $h \equiv 1 \pmod{B}$ ; тогда  $ga + hb$  удовлетворяет сравнениям китайской теоремы об остатках. Следовательно, это утверждение равносильно китайской теореме об остатках.

Рассмотрим сначала случай, когда  $A$  и  $B$  — простые дивизоры. Если они делят различные простые целые числа, например  $p_A$  и  $p_B$ , где  $p_A \neq p_B$ , то, по обычной китайской теореме об остатках для целых чисел, имеется целое число  $k$ , удовлетворяющее сравнениям  $k \equiv 1 \pmod{p_A}$  и  $k \equiv 0 \pmod{p_B}$ . Тогда  $k \equiv 1 \pmod{A}$  и  $k \equiv 0 \pmod{B}$ , как и требуется. Если  $p_A = p_B$ , то, в частности,  $p_A \neq \lambda$ , поскольку  $\lambda$  имеет только один простой дивизор, а по предположению  $A \neq B$ . Тогда, по теореме из § 4.12, имеется круговое целое  $\psi$ , которое удовлетворяет условиям  $\psi \equiv 0 \pmod{B}$  и  $\psi \not\equiv 0 \pmod{A}$ . Далее, так как  $A$  простой, то *ненулевые элементы обратимы по модулю  $A$* , т. е. из  $\psi \not\equiv 0 \pmod{A}$  вытекает наличие такого  $\varphi$ , что  $\psi\varphi \equiv 1 \pmod{A}$ . Это можно доказать следующим образом. Пусть  $a_1, a_2, \dots, a_v$ , где  $v = p_A^f$ , есть полная система представителей по модулю  $A$ , т. е. система таких круговых целых, что каждое круговое целое сравнимо по модулю  $A$  с одним и только одним из  $a_i$ . Тогда  $\psi a_1, \psi a_2, \dots, \psi a_v$  все различны по модулю  $A$ , поскольку из  $\psi a_i \equiv \psi a_j \pmod{A}$  вытекает  $\psi(a_i - a_j) \equiv 0 \pmod{A}$ , откуда, так как  $\psi \not\equiv 0 \pmod{A}$  и  $A$  простой, имеем  $a_i - a_j \equiv 0 \pmod{A}$  и, следовательно,  $a_i = a_j$ . Поскольку каждое  $\psi a_i$  сравнимо с одним и только одним из  $a_j$  и никакие два из них не сравнимы с одним и тем же  $a_j$ , каждое  $a_j$  сравнимо с одним и только одним из  $\psi a_i$ , и, в частности, единица 1 сравнима с  $\psi a_i$  при некотором  $i$ . Тогда  $\psi a_i \equiv 1 \pmod{A}$  и  $\psi a_i \equiv 0 \pmod{B}$ , что и требуется.

Рассмотрим теперь случай, когда  $A$  и  $B$  — степени простых, например  $A = P^n$ ,  $B = Q^m$ , где  $P$  и  $Q$  — различные простые дивизоры, а  $n$  и  $m$  — положительные целые числа. На основании доказанного выше имеется такое круговое целое  $g$ , что  $g \equiv 1 \pmod{P}$  и  $g \equiv 0 \pmod{Q}$ . Пусть  $h = g^m$ . Тогда  $h \equiv 0 \pmod{B}$ . По модулю  $A$  мы можем написать сравнение  $h \equiv a_0 + a_1\psi + \dots + a_{n-1}\psi^{n-1}$ , где  $\psi$  делится на  $P$  с кратностью точно 1 и не делится ни на один дивизор, сопряженный дивизору  $P$ . Кроме того, поскольку  $h \equiv 1 \pmod{P}$ , имеем  $a_0 \equiv 1 \pmod{P}$ , и в приведенном ранее построении элемента  $a_0 + a_1\psi + \dots + a_{n-1}\psi^{n-1}$  можно положить  $a_0 = 1$  и найти значения  $a_1, a_2, \dots, a_{n-1}$ . Затем можно найти такое круговое целое  $f$ , для которого  $hf \equiv 1 \pmod{A}$ , написав  $f = b_0 + b_1\psi + \dots + b_{n-1}\psi^{n-1}$ ,  $hf \equiv b_0 + (b_1 + a_1b_0)\psi + (b_2 + a_1b_1 + a_2b_0)\psi^2 + \dots + (b_{n-1} + a_1b_{n-2} + \dots + a_{n-1}b_0)\psi^{n-1} \pmod{A}$  и воспользовавшись уравнениями  $b_0 = 1, b_1 + a_1b_0 = 0, b_2 + a_1b_1 + a_2b_0 = 0, \dots, b_{n-1} + a_1b_{n-2} + \dots + a_{n-1}b_0 = 0$  для последовательного



определения неизвестных  $b_0, b_1, b_2, \dots, b_{n-1}$ . Тогда, как и требуется,  $hf \equiv 1 \pmod{A}$ ,  $hf \equiv 0 \pmod{B}$ .

Рассмотрим, наконец, случай, когда  $A = A_1 A_2 \dots A_\mu$ ,  $B = B_1 B_2 \dots B_\nu$ , где  $A_i$  и  $B_j$  все являются попарно взаимно простыми степенями простых дивизоров. Тогда, как уже показано, для  $C = A_2, A_3, \dots, A_\mu, B_1, B_2, \dots, B_\nu$  имеется такое круговое целое, которое есть 1 по модулю  $A_1$  и 0 по модулю  $C$ . Произведение этих  $\mu + \nu - 1$  круговых целых есть 1 по модулю  $A_1$  и 0 по модулю  $A_2, A_3, \dots, A_\mu, B_1, B_2, \dots, B_\nu$ . Пусть  $g_1$  обозначает это круговое целое. Таким же способом можно найти круговые целые  $g_2, g_3, \dots, g_\mu$ , обладающие свойствами:  $g_i \equiv 1 \pmod{A_i}$ , но  $g_i \equiv 0$  по модулю всех дивизоров  $A_1, \dots, A_\mu, B_1, \dots, B_\nu$ , отличных от  $A_i$ . Тогда круговое целое  $g_1 + g_2 + \dots + g_\mu$  есть 1 по модулю каждого из  $A_1, A_2, \dots, A_\mu$  и, следовательно, оно есть 1 по модулю  $A$ , в то время как по модулю каждого из  $B_1, B_2, \dots, B_\nu$  оно есть 0 и, следовательно, оно есть 0 по модулю  $B$ . Это завершает доказательство китайской теоремы об остатках.

## Упражнения

1. Докажите предложение 1. [Покажите, что для этого будет достаточно доказать, что из  $g(\alpha) \equiv 0 \pmod{\sigma A}$  вытекает  $\sigma^{-1}g(\alpha) \equiv 0 \pmod{A}$ . Докажите это прямым путем в случае, когда  $A$  есть степень простого дивизора. Затем выведите общий случай.]

2. Докажите предложение 2.

3. Докажите следующее обобщение того факта, что наибольший общий делитель  $d$  двух целых чисел  $m$  и  $n$  может быть записан в виде  $d = at + bn$  при некоторых целых  $a$  и  $b$ : если  $g_1(\alpha), g_2(\alpha), \dots, g_n(\alpha)$  — данные круговые целые, то круговое целое  $\varphi(\alpha)$  тогда и только тогда можно записать в виде  $\varphi(\alpha) = b_1(\alpha)g_1(\alpha) + b_2(\alpha)g_2(\alpha) + \dots + b_n(\alpha)g_n(\alpha)$ , когда оно делится на наибольший общий дивизор данных  $g_1(\alpha), g_2(\alpha), \dots, g_n(\alpha)$ . Вместе с упр. 2 предыдущего параграфа это доказывает теорему Дедекинда о том, что «идеалы» могут быть описаны как при помощи свойств (i) и (ii), так и при помощи дивизоров. [Ясно, что если  $\varphi$  есть комбинация данных  $g_i$ , то  $\varphi$  делится на их н. о. д. Требуется доказать обратное. Если  $n = 1$ , то это есть основная теорема. Покажите, что если это верно для  $n - 1$ , то верно и для  $n$ . Пусть  $A$  — н. о. д., и пусть  $AB$  — н. о. д. первых  $n - 1$  из данных  $g_i$ . Требуется доказать, что если  $\varphi(\alpha) \equiv 0 \pmod{A}$ , то сравнение  $\varphi(\alpha) \equiv b_n(\alpha)g_n(\alpha) \pmod{AB}$  можно решить относительно  $b_n(\alpha)$ . Докажите это рассмотрением степеней простых дивизоров, расчленив на них  $AB$  и применяя китайскую теорему об остатках.]

## 4.15. Выводы

Теория дивизоров может быть описана как отображение

$$\left\{ \begin{array}{l} \text{ненулевые} \\ \text{круговые} \\ \text{целые} \end{array} \right\} \rightarrow \{\text{дивизоры}\}$$

Главным этапом в построении теории является определение *простых* дивизоров. Каждый простой дивизор делит простое число  $p$ ; простое число  $\lambda$  имеет один простой дивизор, а простое  $p \neq \lambda$  имеет  $e$  простых дивизоров, где  $ef = \lambda - 1$  и  $f$  — показатель числа  $p$  по модулю  $\lambda$ . Дивизор — это любое произведение простых дивизоров. Таким образом, *по определению*, для дивизоров выполняется единственность разложения на простые. Отображение, обозначенное выше стрелкой, ставит в соответствие каждому круговому целому его дивизор, т. е. делящие его простые дивизоры, подсчитанные с кратностями. Вот основные свойства этого отображения:

(i) Дивизор числа  $\lambda$  есть  $(\lambda - 1)$ -я степень делящего его простого дивизора. Если  $p$  — другое простое целое число, то дивизор числа  $p$  есть произведение  $e$  делящих его простых дивизоров (каждый входит в произведение в первой степени).

(ii) Дивизор произведения есть произведение дивизоров.

(iii) Если сравнение  $g_1(\alpha) \equiv g_2(\alpha) \pmod{A}$  определено условием: дивизор элемента  $g_1(\alpha) - g_2(\alpha)$  делится на  $A$  (где  $g_1(\alpha)$ ,  $g_2(\alpha)$  — круговые целые, а  $A$  — дивизор), то это отношение сравнимости обладает обычными свойствами, т. е. рефлексивно, симметрично, транзитивно и согласовано со сложением и умножением.

(iv) Два дивизора, определяющие одну и ту же сравнимость в смысле (iii), с необходимостью идентичны.

(v) Основная теорема: если дивизор элемента  $g(\alpha)$  делит дивизор элемента  $h(\alpha)$ , то  $g(\alpha)$  делит  $h(\alpha)$ .

Из основной теоремы следует, что *два круговых целых, которые имеют один и тот же дивизор, совпадают с точностью до сомножителя, являющегося единицей*. Таким образом, если пренебречь единицами в качестве сомножителей, то круговые целые определяются своими дивизорами. Дивизор можно рассматривать как «разложение» кругового целого, но на простые дивизоры, а не на простые круговые целые. Если каждый простой дивизор есть дивизор кругового целого, т. е. если приведенное выше отображение есть отображение *на* множество всех дивизоров, то единственность разложения на простые круговые целые выполняется (упр. 1). Однако при  $\lambda = 23$  простые дивизоры числа  $p = 47$  не являются дивизорами никакого кругового целого. В этом случае, а также в любом случае, когда имеется простой дивизор, не являющийся дивизором кругового целого, единственность разложения на простые круговые целые *нарушается* (упр. 2).

Дальнейшее изучение разложения круговых целых опирается на изучение вопроса: «Какие дивизоры являются дивизорами

круговых целых?», или, иными словами, «Что является *образом* приведенного выше отображения?». Это и есть предмет следующей главы.

## Упражнения

1. Покажите, что указанное отображение тогда и только тогда является отображением на множество всех дивизоров, когда каждый простой дивизор есть дивизор некоторого кругового целого. Покажите, что, когда это так, каждое круговое целое может быть записано как произведение простых круговых целых, и два таких разложения данного кругового целого совпадают с точностью до сомножителей, являющихся единицами.

2. Покажите, что если имеется простой дивизор, не являющийся дивизором кругового целого, то найдется круговое целое, которое не делится ни на какое простое круговое целое. Покажите сверх того, что в этом случае имеется круговое целое, которое может быть разложено в произведение неразложимых круговых целых двумя различными способами, причем различие сохранится, даже если пренебрегать сомножителями, являющимися единицами. [Используйте круговое целое  $\psi$  ( $\eta$ ), которое делится на точно один простой дивизор числа  $p$  с кратностью точно 1.]

## Глава 5

# ПОСЛЕДНЯЯ ТЕОРЕМА ФЕРМА ДЛЯ РЕГУЛЯРНЫХ ПРОСТЫХ

### 5.1. Замечания Куммера о квадратичных целых

Крупные нововведения часто совершаются не сторонниками радикальных изменений, а людьми, которые питают большое почтение к тому, что сделано раньше, и руководствуются желанием хранить и продолжать традиции своих предшественников. Именно так обстояло дело в случае с Куммером. Как указывает К.-Р. Бирманн в написанной им биографии Куммера (Dictionary of Scientific Biography), Куммер по характеру был очень консервативен, но не в каком-то узком политическом смысле, а в том смысле, что он был предан созиданию на основе существующих традиций. Чтобы правильно понять побуждения деятельности Куммера, важно уяснить, что он не имел намерений вводить новые абстрактные структуры ради них самих; напротив, как он говорит в начале сообщения [К7] по своей новой теории, его целью были «дополнение и упрощение» существующих структур.

Эта глава посвящена доказательству Куммером Последней теоремы Ферма для широкого класса простых показателей  $\lambda$ , которые сейчас известны как *регулярные* простые. Это доказательство требует еще одного важного сделанного Куммером нововведения, а именно, понятия *эквивалентности* двух дивизоров (двух идеальных комплексных чисел). Имея в виду личность Куммера, нужно думать, что это новое понятие эквивалентности было обусловлено неким весьма существенным соображением; Куммер не стал бы вводить его лишь потому, что это было бы «интересной» возможностью. Хотя соблазнительно предположить, что определение эквивалентности дивизоров было обусловлено настойчивой попыткой доказать Последнюю теорему Ферма, в действительности оно было включено в качестве весьма важной части в куммерово первоначальное сообщение по теории идеальных делителей в 1846 г., заведомо до поспешной публикации Ламе, подтолкнувшей Куммера к подробному развитию выводов своей теории для Последней теоремы Ферма. Поэтому вряд ли эта деятельность играла главную роль как источник первоначального определения эквивалентности.

По-видимому, по крайней мере два соображения обусловили это определение. Во-первых, при применении теории дивизоров к реальным задачам — например, задачам о круговых целых,

которые Куммер рассматривает в своем сообщении 1846 г., — приходится почти сразу столкнуться с вопросом: «Когда данный дивизор является дивизором реально существующего кругового целого?». Решение этого вопроса, как будет показано в следующем параграфе, совершенно естественно приводит к понятию эквивалентности. Второе соображение, как это явствует из высказываний самого Куммера, было для него почти столь же важным, как и первое. Дело в том, что это понятие эквивалентности очень тесно связано с гауссовым понятием эквивалентности квадратичных форм.

И вот опять появляется возможность объяснить нововведение Куммера его «консервативностью». Изучение уравнения Пелля и других уравнений второй степени с двумя неизвестными совершенно естественно приводит к понятию *эквивалентности* бинарных квадратичных форм (см. § 8.2). Гаусс в *Disquisitiones Arithmeticae* ввел более сильное понятие *собственной эквивалентности* (см. § 8.3). Куммер замечает, что в теории бинарных квадратичных форм это понятие всегда кажется натянутым и искусственным — оно требует, например, считать, две формы  $ax^2 + 2bxy + cy^2$  и  $cx^2 + 2bxy + ay^2$  не эквивалентными в собственном смысле, несмотря на то, что «нужно признать гауссову классификацию точнее отражающей существо дела». Таким образом, неявно заключает Куммер, гауссово понятие собственной эквивалентности нужно *спасти* от этой искусственности. Он говорит, что теория идеальной факторизации выполняет эту роль, поскольку «всю теорию бинарных квадратичных форм можно интерпретировать как теорию комплексных чисел вида  $x + y\sqrt{D}$  ( $D$  — гауссово обозначение *детерминанта*  $b^2 - ac$  квадратичной формы  $ax^2 + 2bxy + cy^2$ ) и в результате такой интерпретации эта теория с необходимостью приводит к идеальным комплексным числам (дивизорам) такого же типа». Далее он, по существу, говорит, что понятие эквивалентности, определенное им для идеальных комплексных чисел вида  $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-1}\alpha^{\lambda-1}$ , применимо и к идеальным комплексным числам вида  $x + y\sqrt{D}$ , и, когда последние интерпретируются как бинарные квадратичные формы, это понятие эквивалентности совпадает с гауссовым понятием собственной эквивалентности. Это и есть, как он заключает, «истинный смысл» гауссова понятия.

Совершенно таинственным выглядит то, что Куммер *никогда не публиковал* никаких подробностей этой связи между бинарными квадратичными формами и идеальными комплексными числами (дивизорами) вида  $x + y\sqrt{D}$ . Несколько нечетких замечаний в его сообщении 1846 г. и еще несколько отрывочных указаний в более поздних трактатах ([K8], стр. 366, и [K11], стр. 114) — вот и все, что он сказал по этому поводу, или, во всяком случае,

все, что сохранилось. Таким образом, хотя кажется вполне определенным, что аналогия с гауссовой теорией сыграла некоторую роль в возникновении понятия эквивалентности дивизоров, точную роль этой аналогии мы уже не сможем установить. В § 5.2 и 5.3 понятие эквивалентности дивизоров развивается без каких бы то ни было ссылок на гауссову теорию, однако, как будет видно в гл. 7 и 8, центральный вопрос § 5.2 очень тесно связан с ней. По моему личному мнению, приводимое здесь изложение очень близко к тому, которому в действительности следовал Куммер, но я берусь утверждать лишь то, что такой подход делает понятие эквивалентности весьма естественным и полезным.

В дальнейших параграфах этой главы даются два приложения теории Куммера. Первое, более важное из них, представляет собой доказательство Последней теоремы Ферма для всех простых показателей  $\lambda$ , которые удовлетворяют некоторым условиям (A) и (B). Вторым является доказательство знаменитого закона взаимности. Это доказательство следует рассматривать скорее как некое отступление. Оно является естественным продолжением хода рассуждений § 5.2, которые приводят не только к доказательству закона квадратичной взаимности, но даже к открытию *формулировки* этого закона. Однако здесь это оказывается полным анахронизмом, поскольку работа Куммера вышла через 50 лет после появления первого доказательства квадратичной взаимности, и это приложение его теории, насколько мы знаем, не рассматривалось Куммером.

## 5.2. Эквивалентность дивизоров в частном случае

В своем сообщении 1846 г. по теории идеальной факторизации Куммер говорит, что его определение «эквивалентности» для идеальных комплексных чисел (дивизоров) может быть переформулировано и применено к частному случаю так, чтобы дать определение «эквивалентности» для некоторых бинарных квадратичных форм детерминанта  $\lambda$ , и что когда это будет сделано, полученное определение совпадет с гауссовым определением *собственной* эквивалентности. Можно не сомневаться, что частный случай, который имел в виду Куммер, был случаем тех круговых целых, которые в обозначениях гл. 4 имеют вид  $a + b\theta_0 + c\theta_1$ . (Здесь  $\theta_0, \theta_1$  — два периода длины  $(\lambda - 1)/2$  и  $a, b, c$  — целые числа.) Для квадратичных целых этого вида норма  $N(a + b\theta_0 + c\theta_1)$  представляет собой, по существу, бинарную квадратичную форму, а это и устанавливает связь между круговыми целыми и гауссовой теорией.

Как было указано в гл. 4, основной вопрос, который приводит к введению понятия эквивалентности, — это вопрос: *какие дивизоры являются дивизорами круговых целых*, т. е. каков образ ото-



бражения из § 4.15? В этом параграфе рассматривается один частный случай этой задачи, а именно: *какие дивизоры являются дивизорами круговых целых вида  $a + b\theta_0 + c\theta_1$  при  $\lambda = 23$ ?* (Здесь  $\theta_0$  и  $\theta_1$  — два периода длины 11, причем  $\theta_0$  — тот из них, который содержит  $\alpha$ , а  $\theta_1$  — другой. Таким образом,  $1 + \theta_0 + \theta_1 = 0$ ,  $\theta_0 = \alpha + \alpha^4 + \alpha^{-7} + \alpha^{-5} + \alpha^3 + \alpha^{-11} + \alpha^2 + \alpha^8 + \alpha^9 + \alpha^{-10} + \alpha^6$  и  $\theta_1 = \alpha^{-2} + \alpha^{-8} + \dots + \alpha^{11}$ .) Изучение этого частного случая естественным путем приведет к идее эквивалентности дивизоров.

Первый полезный шаг при решении нашей задачи — составить достаточно большой список круговых целых вида  $a + b\theta_0 + c\theta_1$  и их дивизоров. Благодаря условию  $1 + \theta_0 + \theta_1 = 0$  каждое такое круговое целое может быть записано в виде  $a + b\theta_0$ . Его норма есть произведение 22 сомножителей, 11 из которых равны  $a + b\theta_0$ , а остальные 11 равны  $a + b\theta_1$ ; таким образом, эта норма является 11-й степенью числа  $(a + b\theta_0)(a + b\theta_1) = a^2 + ab(\theta_0 + \theta_1) + b^2\theta_0\theta_1 = a^2 - ab + 6b^2$ . (Равенство  $\theta_0\theta_1 = 6$  при  $\lambda = 23$  было отмечено в § 4.4.) Именно то обстоятельство, что норма числа  $a + b\theta_0$  так тесно связана с бинарной квадратичной формой  $a^2 - ab + 6b^2$ , и обеспечивает связь между этим частным случаем теории Куммера и теорией Гаусса. Подробнее об этой связи, которая в этом параграфе не играет роли, см. гл. 7 и 8.

Таблица 5.2.1 содержит список значений формы  $a^2 - ab + 6b^2$  для различных значений коэффициентов  $a$  и  $b$ . (Для каждого положительного  $a$  даны все положительные  $b$ , взаимно простые с  $a$ , для которых  $a^2 - ab + 6b^2 < 150$ .) Используя этот список, легко заполнить список дивизоров соответствующих круговых целых  $a + b\theta_0$ . Например, первая строка  $(1 + \theta_0)(1 + \theta_1) = 2 \cdot 3$  таблицы показывает, что каждый простой дивизор сомножителя 2 делит произведение  $(1 + \theta_0)(1 + \theta_1)$  с кратностью точно 1 и, следовательно, делит либо  $1 + \theta_0$ , либо  $1 + \theta_1$ , но не оба эти числа. Если он делит  $1 + \theta_0$ , то его сопряженный, полученный заменой  $\alpha \mapsto \alpha^{-2}$ , делит  $1 + \theta_1$ , и наоборот. Следовательно, число простых дивизоров сомножителя 2 должно быть четным, причем половина из них делит  $1 + \theta_0$ , а остальные делят  $1 + \theta_1$ . (На самом же деле легко видеть, что показатель числа 2 по модулю 23 есть 11, так что 2 имеет точно два простых дивизора. Однако эти более подробные сведения в дальнейшем не понадобятся.)

В табл. 5.2.2 символ  $(2, 1)$  обозначает дивизор, являющийся произведением всех простых дивизоров числа 2, которые делят  $1 + \theta_0$ . Аналогично, число 3 должно иметь четное число простых дивизоров, половина из которых делит  $1 + \theta_0$ , а вторая половина делит  $1 + \theta_1$ . По соображениям, которые вскоре будут объяснены, символ  $(3, -1)$  обозначает произведение тех простых дивизоров числа 3, которые делят  $1 + \theta_0$ . Равенство  $(1 + \theta_0)(1 + \theta_1) = 2 \cdot 3$  показывает, что никакой простой дивизор простых чисел  $p$ ,

отличных от 2 и 3, не делит  $1 + \theta_0$  и что все простые дивизоры, делящие это число, имеют кратность точно 1; поэтому ясно, что  $(2, 1) (3, -1)$  есть дивизор числа  $1 + \theta_0$ , как и указано в табл. 5.2.2.

Вторая строка в таблице особая, потому что она касается особого простого числа 23, которое в отличие от остальных,

Таблица 5.2.1

$a$	$b$	$(a + b\theta_0)(a + b\theta_1)$	$a$	$b$	$(a + b\theta_0)(a + b\theta_1)$
1	1	$6 = 2 \cdot 3$	5	4	$101 = \text{простое}$
1	2	$23 = \text{простое}$	6	1	$36 = 2^2 \cdot 3^2$
1	3	$52 = 2^2 \cdot 13$	6	5	$156 = 2^2 \cdot 3 \cdot 13$
1	4	$93 = 3 \cdot 31$	7	1	$48 = 2^4 \cdot 3$
1	5	$146 = 2 \cdot 73$	7	2	$59 = \text{простое}$
2	1	$8 = 2^3$	7	3	$82 = 2 \cdot 41$
2	3	$52 = 2^2 \cdot 13$	7	4	$117 = 3^2 \cdot 13$
2	5	$144 = 2^4 \cdot 3^2$	8	1	$62 = 2 \cdot 31$
3	1	$12 = 2^2 \cdot 3$	8	3	$94 = 2 \cdot 47$
3	2	$27 = 3^3$	9	1	$78 = 2 \cdot 3 \cdot 13$
3	4	$93 = 3 \cdot 31$	9	2	$87 = 3 \cdot 29$
3	5	$144 = 2^4 \cdot 3^2$	9	4	$141 = 3 \cdot 47$
4	1	$18 = 2 \cdot 3^2$	10	1	$96 = 2^5 \cdot 3$
4	3	$58 = 2 \cdot 29$	10	3	$124 = 2^2 \cdot 31$
4	5	$146 = 2 \cdot 73$	11	1	$116 = 2^2 \cdot 29$
5	1	$26 = 2 \cdot 13$	11	2	$123 = 3 \cdot 41$
5	2	$39 = 3 \cdot 13$	11	3	$142 = 2 \cdot 71$
5	3	$64 = 2^6$	12	1	$138 = 2 \cdot 3 \cdot 23$

имеющих дивизор, разложимый в произведение различных простых дивизоров, имеет дивизором 22-ю степень одного дивизора  $(\alpha - 1)$ . Так как норма числа  $1 + 2\theta_0$  равна  $23^{11}$ , то его дивизор есть некоторая степень дивизора  $(\alpha - 1)$ , а именно 11-я степень, как и указано в табл. 5.2.2.

По третьей строке удобнее всего объяснить обозначения. Из  $(1 + 3\theta_0)(1 + 3\theta_1) = 2^2 \cdot 13$  следует, что каждый простой дивизор числа 2 делит либо  $1 + 3\theta_0$ , либо  $1 + 3\theta_1$ . Никакой из этих простых дивизоров не может делить оба эти элемента, ибо тогда он делил бы их сумму  $2 + 3\theta_0 + 3\theta_1 = -1$ , что невозможно. Таким образом, число 2 должно иметь четное число простых дивизоров, половина которых делит  $1 + 3\theta_0$ , а вторая половина

Таблица 5.2.2

Круговое целое	Дивизор	Круговое целое	Дивизор
$1 + \theta_0$	$(2, 1)(3, -1)$	$5 + 4\theta_0$	$(101, 24)$
$1 + 2\theta_0$	$(\alpha - 1)$	$6 + \theta_0$	$(2, 0)^2(3, 0)^2$
$1 + 3\theta_0$	$(2, 1)^2(13, 4)$	$6 + 5\theta_0$	$(2, 0)^2(3, 0)(13, 4)$
$1 + 4\theta_0$	$(3, -1)(31, -8)$	$7 + \theta_0$	$(2, 1)^4(3, -1)$
$1 + 5\theta_0$	$(2, 1)(73, 29)$	$7 + 2\theta_0$	$(59, 26)$
$2 + \theta_0$	$(2, 0)^3$	$7 + 3\theta_0$	$(2, 1)(41, -16)$
$2 + 3\theta_0$	$(2, 0)^2(13, -5)$	$7 + 4\theta_0$	$(3, -1)^2(13, -5)$
$2 + 5\theta_0$	$(2, 0)^4(3, -1)^2$	$8 + \theta_0$	$(2, 0)(31, -8)$
$3 + \theta_0$	$(2, 1)^2(3, 0)$	$8 + 3\theta_0$	$(2, 0)(47, 13)$
$3 + 2\theta_0$	$(3, 0)^3$	$9 + \theta_0$	$(2, 1)(3, 0)(13, 4)$
$3 + 4\theta_0$	$(3, 0)(31, 7)$	$9 + 2\theta_0$	$(3, 0)(29, 10)$
$3 + 5\theta_0$	$(2, 1)^4(3, 0)^2$	$9 + 4\theta_0$	$(3, 0)(47, -14)$
$4 + \theta_0$	$(2, 0)(3, -1)^2$	$10 + \theta_0$	$(2, 0)^5(3, -1)$
$4 + 3\theta_0$	$(2, 0)(29, -11)$	$10 + 3\theta_0$	$(2, 0)^2(31, 7)$
$4 + 5\theta_0$	$(2, 0)(73, -30)$	$11 + \theta_0$	$(2, 1)^2(29, -11)$
$5 + \theta_0$	$(2, 1)(13, -5)$	$11 + 2\theta_0$	$(3, -1)(41, 15)$
$5 + 2\theta_0$	$(3, -1)(13, 4)$	$11 + 3\theta_0$	$(2, 1)(71, 20)$
$5 + 3\theta_0$	$(2, 1)^6$	$12 + \theta_0$	$(2, 0)(3, 0)(\alpha - 1)^{11}$

делит  $1 + 3\theta_1$ . Это разделение простых дивизоров числа 2 должно быть точно таким же, как в первой строке, поскольку если  $P$  — простой дивизор числа 2, то  $2 \equiv 0 \pmod{P}$ ,  $2\theta_0 \equiv 0 \pmod{P}$ , и, значит,  $P$  тогда и только тогда делит  $1 + \theta_0$ , когда он делит  $1 + \theta_0 + 2\theta_0 = 1 + 3\theta_0$ . В других строках таблицы, таких, как  $(1 + 5\theta_0)$   $(1 + 5\theta_1)$ ,  $(2 + \theta_0)$   $(2 + \theta_1)$ ,  $(4 + 3\theta_0)$   $(4 + 3\theta_1)$  и т. д., имеет место такое же разделение простых дивизоров числа 2 на два подмножества. Чтобы придумать обозначения для тех двух сомножителей, на которые во всех этих случаях разлагается число 2, естественно заметить, что и  $\theta_0$  и  $\theta_1$ , как видно из уравнения для  $\theta_i$ , по модулю любого простого дивизора числа 2 сравнимы с целыми числами и в соответствии с этими целыми числами и происходит разделение среди простых дивизоров. Например, если  $P$  есть простой дивизор числа 2, делящий  $1 + \theta_0$ , то  $1 + \theta_0 \equiv 0 \pmod{P}$ ,  $\theta_0 \equiv -1 \equiv 1 \pmod{P}$ ,  $\theta_1 = -1 - \theta_0 \equiv -1 - 1 \equiv 0 \pmod{P}$ . С другой стороны, если  $P$  делит  $1 + \theta_1$ , то  $\theta_0 \equiv 0$ ,

$\theta_1 \equiv 1 \pmod{P}$ . Значит, в первом случае  $3 + \theta_0 \equiv 3 + 1 \equiv 0 \pmod{P}$ , а во втором случае  $3 + \theta_0 \equiv 3 + 0 \not\equiv 0 \pmod{P}$ , так что  $P$  делит  $3 + \theta_0$  в первом случае, но не делит во втором. Если через  $(2, 1)$  обозначено произведение тех простых дивизоров числа 2, по модулю которых  $\theta_0 \equiv 1$ , то каждый простой сомножитель дивизора  $(2, 1)$  делит  $1 + 3\theta_0$  с кратностью точно 2, поскольку он не делит  $1 + 3\theta_1$  ( $1 + 3 \cdot 0 = 1 \not\equiv 0$ ), но делит  $(1 + 3\theta_0) \times \times (1 + 3\theta_1)$  с кратностью точно 2. Простые дивизоры числа 13 делят  $1 + 3\theta_0$  или  $1 + 3\theta_1$ , но не оба эти элемента. Делящие  $1 + 3\theta_0$  — это те, по модулю которых  $1 + 3\theta_0 \equiv 0$ ,  $4 + 12\theta_0 \equiv 0$ ,  $4 - \theta_0 \equiv 0$ ,  $\theta_0 \equiv 4$ . Такой способ идентификации простых дивизоров позволяет легко определить, что, например, указанные простые дивизоры числа 13 являются теми же самыми, которые делят  $5 + 2\theta_0$  (так как по их модулю  $5 + 2\theta_0 \equiv 5 + 2 \cdot 4 \equiv 13 \equiv 0$ ), и отличны от тех, которые делят  $2 + 3\theta_0$  (так как  $2 + 3\theta_0 \equiv 2 + 3 \cdot 4 \equiv 1 \not\equiv 0$ ). Если через  $(13, 4)$  обозначены простые дивизоры числа 13, по модулю которых  $\theta_0 \equiv 4$ , то дивизор числа  $1 + 3\theta_0$  можно записать в виде  $(2, 1)^2 (13, 4)$ .

Теперь легко понять последующие строки табл. 5.2.2. В каждом случае запись  $(p, u)$  используется для обозначения произведения всех простых дивизоров числа  $p$ , которые делят  $\theta_0 - u$ . Эти дивизоры составляют точно половину простых дивизоров числа  $p$ , поскольку если бы дивизор  $P$  делил как  $\theta_0 - u$ , так и  $\theta_1 - u$ , то его сопряженный, получаемый заменой  $\alpha \mapsto \alpha^{-2}$ , также делил бы оба эти числа, откуда бы вытекало, что и все сопряженные дивизора  $P$  делят оба эти числа; но сопряженные дивизора  $P$  содержат все простые дивизоры числа  $p$ , а это влекло бы за собой, что  $p$  делит как  $\theta_0 - u$ , так и  $\theta_1 - u$ , вопреки тому что  $p$ , очевидно, не делит ни одно из них. (На самом деле легко показать, что дивизоры  $(p, u)$ , встречающиеся в таблице, все являются *простыми* дивизорами, кроме  $(47, 13)$  и  $(47, -14)$ . Этот факт не имеет отношения к рассматриваемой сейчас задаче.)

Таким образом, табл. 5.2.2 дает список большого числа дивизоров, являющихся дивизорами круговых целых вида  $a + b\theta_0 + c\theta_1$ . Число элементов в таблице можно удвоить, если воспользоваться сопряжением  $\alpha \mapsto \alpha^{-2}$ . Эта операция переводит  $\theta_0$  в  $\theta_1 = -1 - \theta_0$ , а дивизор  $(p, u)$  в дивизор  $(p, -1 - u)$ . Таким образом, дивизоры  $(2, 0)$   $(3, 0)$ ,  $(2, 0)^2$   $(13, -5)$ ,  $(3, 0)$   $(31, 7)$ , ... завершают перечень всех дивизоров круговых целых вида  $a + b\theta_0 + c\theta_1$ . (На самом деле число элементов в таблице не вполне удвоится, поскольку  $(\alpha - 1)^{11}$  сопряжен с самим собой.) Дивизор, являющийся дивизором какого-нибудь кругового целого, по причинам исторического характера, которые будут объяснены в § 8.5, называется *главным* дивизором. Здесь дивизор будет называться *главным*, если он есть дивизор кругового целого вида

$a + b\theta_0 + c\theta_1$ . Приведенный выше список главных дивизоров очень длинный, и его легко продолжить дальше. Но наша задача заключается в том, чтобы научиться определять, когда данный дивизор является главным.

Прежде всего имеются очень простые необходимые условия для того, чтобы дивизор  $A$  был главным. Предположим сначала, что  $(\alpha - 1)$  делит  $A$  и что  $A$  есть дивизор элемента  $a + b\theta_0$ . Тогда  $(\alpha - 1)$  делит целое число  $(a + b\theta_0)(a + b\theta_1)$ , откуда следует, что и  $\lambda$  делит  $(a + b\theta_0)(a + b\theta_1)$ , скажем  $(a + b\theta_0)(a + b\theta_1) = \lambda^j k$ , где  $k$  — целое число, не делящееся на  $\lambda$ , и  $j \geq 1$ . Дивизор  $(\alpha - 1)$  делит  $a + b\theta_0$  с кратностью  $\mu$  тогда и только тогда, когда он делит  $a + b\theta_1$  с кратностью  $\mu$ , поэтому  $(\alpha - 1)$  делит  $a + b\theta_0$  с кратностью точно  $11j$ . Таким образом, необходимое условие того, что дивизор  $A$  является главным, заключается в том, что он имеет вид  $A = (\alpha - 1)^{11j} B$ , где  $j \geq 0$ , а дивизор  $B$  не делится на  $(\alpha - 1)$ .

Пусть теперь  $P$  — любой простой дивизор, отличный от исключительного дивизора  $(\alpha - 1)$ , и пусть  $P \mid A$ , где  $A$  — главный дивизор. Пусть  $p$  — простое целое число, которое делится на  $P$ , и пусть  $P_1, P_2, \dots, P_e$  — такие простые дивизоры числа  $p$ , что  $P = P_1 P_{j+1}$  получается из  $P_j$  сопряжением  $\alpha \mapsto \alpha^{-2}$  и  $f = (\lambda - 1)/e$  — показатель числа  $p$  по модулю 23. Так как  $A$  есть дивизор некоторого числа  $a + b\theta_0$ , а это число инвариантно при  $\alpha \mapsto \alpha^4$ , то из предположения  $P_1 \mid A$  вытекает, что все дивизоры  $P_3, P_5, P_7, \dots$  делят  $A$ . Если  $e$  нечетно, то эта последовательность включает все простые дивизоры числа  $p$  и  $A$  делится на дивизор  $(p)$  числа  $p$ . Значит, еще одно необходимое условие того, что дивизор  $A$  является главным, заключается в том, что он имеет вид  $A = (\alpha - 1)^{11j} (p_1) (p_2) \dots (p_k) B$ , где  $B$  — дивизор, все простые дивизоры которого имеют четное число  $e$  сопряженных. Наконец, если  $e$  четно, то произведение  $P_1 P_3 \dots P_{e-1}$  делит  $A$ . Утверждается, что этот дивизор  $P_1 P_3 \dots P_{e-1}$  имеет вид  $(p, u)$ . Для доказательства достаточно заметить, что все периоды длины  $f = 22/e = 22/2k$  сравнимы с целыми числами по модулю  $P_1$  или по модулю любого простого дивизора числа  $p$ . Действительно, по определению,  $k = e/2$ . Так как  $\theta_0$  и  $\theta_1$  являются периодами длины  $11 = k(22/2k) = kf$ , то они оказываются суммами  $k$  периодов длины  $f$  и поэтому сравнимы с целыми рациональными числами по модулю  $P_1$ , скажем  $\theta_0 \equiv u \pmod{P_1}$ . Тогда и все дивизоры  $P_1, P_3, \dots, P_{e-1}$  делят  $\theta_0 - u$ . С другой стороны, ни один из дивизоров  $P_2, P_4, \dots, P_e$  не делит  $\theta_0 - u$ , ибо если бы это число делил один из них, то делили бы и все, а тогда бы  $p \mid (\theta_0 - u)$ , что невозможно.

Отсюда видно, что необходимое условие того, что дивизор  $A$  является главным, заключается в возможности записать его в виде  $A = (\alpha - 1)^{11j} (p'_1) (p'_2) \dots (p'_r) (p_1, u_1) \cdot (p_2, u_2) \dots (p_s, u_s)$ , где

$j$  — неотрицательное целое число,  $p'_1, p'_2, \dots, p'_r$  — простые <sup>1)</sup>, а  $(p_i, u_i)$  при  $i = 1, 2, \dots, s$  обозначает произведение тех простых дивизоров числа  $p_i$ , которые делят  $\theta_0 - u_i$ , причем целые  $p_i$  и  $u_i$  таковы, что  $p_i$  — простое с четным числом простых дивизоров, ровно половина которых делит число  $\theta_0 - u_i$ . Далее, ясно, что дивизор  $(\alpha - 1)^{11j} (p'_1) (p'_2) \dots (p'_r)$  главный, поскольку это есть дивизор элемента  $(1 + 2\theta_0)^j p'_1 p'_2 \dots p'_r$ . Таким образом, если  $(p_1, u_1) (p_2, u_2) \dots (p_s, u_s)$  есть главный дивизор, то умножение элемента  $a + b\theta_0$ , дивизором которого он является, на  $(1 + 2\theta_0)^j p'_1 p'_2 \dots p'_r$  показывает, что дивизор  $A$  главный. Обратно, если  $A$  есть главный дивизор, скажем элемента  $a + b\theta_0$ , то, по основной теореме, произведение  $(1 + 2\theta_0)^j p'_1 p'_2 \dots p'_r$  делит  $a + b\theta_0$ ; кроме того, частное имеет дивизором  $(p_1, u_1) \times \times (p_2, u_2) \dots (p_s, u_s)$  и является элементом вида  $c + d\theta_0$ , поскольку его можно получить умножением на  $(1 + 2\theta_1)^j$ , а затем делением на  $\lambda^j p'_1 p'_2 \dots p'_r$ . Короче,  $A$  является главным тогда и только тогда, когда  $(p_1, u_1) (p_2, u_2) \dots (p_s, u_s)$  является главным дивизором. Существо задачи, следовательно, состоит в том, чтобы *определить, какие дивизоры вида  $(p_1, u_1) (p_2, u_2) \dots (p_s, u_s)$  являются главными.*

Исследование таблицы главных дивизоров пока не позволяет сделать никаких очевидных выводов. Разумно было бы составить список дивизоров, заведомо *не являющихся* главными, с тем чтобы проследить, как они дополняют списки главных дивизоров. В § 4.4 уже было отмечено, что равенство  $(a + b\theta_0) (a + b\theta_1) = 47$  невозможно. Отсюда вытекает, что дивизоры  $(47, 13)$  и  $(47, -14)$  не являются главными. Проще всего установить это, заметив, что равенство  $(a + b\theta_0) (a + b\theta_1) = 2$  невозможно (из него вытекало бы  $a^2 - ab + 6b^2 = 2$ ,  $4a^2 - 4ab + 24b^2 = 8$ ,  $(2a - b)^2 + 23b^2 = 8$ , что, очевидно, невозможно) и, следовательно, дивизор  $(2, 0)$  не является главным. Действительно, если бы  $(2, 0)$  был дивизором числа  $a + b\theta_0$ , то число  $(a + b\theta_0) (a + b\theta_1)$  имело бы тот же дивизор, что и число 2, и было бы целым положительным числом (поскольку его 11-я степень есть норма кругового целого и, следовательно, положительна). Далее, из того, что  $(2, 0)$  — не главный дивизор, но  $(2, 0) (47, 13)$  — главный (см. табл. 5.2.2), следует, что дивизор  $(47, 13)$  — не главный: если бы  $(47, 13)$  был дивизором числа  $a + b\theta_0$ , то  $a + b\theta_0$  делило бы  $8 + 3\theta_0$  и частное  $(8 + 3\theta_0)/(a + b\theta_0) = (8 + 3\theta_0) (a + b\theta_1)/47$  имело бы дивизором  $(2, 0)$ , что невозможно. Таким же способом получаем, что, вообще, если  $A$  — такой дивизор, что  $(2, 0) A$  —

<sup>1)</sup> Можно было бы сделать дополнительное предположение, что все  $p'_1, \dots, p'_r$  имеют нечетное число простых дивизоров, но случай дивизора  $(p')$ , где  $p'$  имеет четное число простых дивизоров, т. е.  $(p') = (p', u) (p', -1 - u)$ , может быть получен за счет перераспределения сомножителей в разложении дивизора  $A$ , а это лишь упрощает задачу.



главный, то  $A$  не может быть главным. При помощи табл. 5.2.2 можно сразу выписать неглавные дивизоры, которые приведены в табл. 5.2.3.

Сходным образом, если  $(2, 1)$   $A$  — главный дивизор, то дивизор  $A$  не является главным. Это дает другой список неглавных дивизоров, которые оказываются сопряженными дивизорам из табл. 5.2.3. Точно так же, поскольку дивизор  $(3, 0)$  не главный,

Таблица 5.2.3

$(3, 0)$	$(2, 0)^5$
$(2, 0)(13, -5)$	$(2, 0)(3, 0)^2$
$(73, -30)$	$(2, 0)(3, 0)(13, 4)$
$(2, 0)^2$	$(2, 0)^3(3, 0)$
$(2, 0)(13, -5)$	$(41, 15)$
$(2, 0)^3(3, -1)^2$	$(31, -8)$
$(2, 0)(3, -1)$	$(47, 13)$
$(2, 0)^3(3, -1)^2$	$(3, -1)(13, -5)$
$(3, -1)^2$	$(2, 0)^4(3, -1)$
$(29, -11)$	$(2, 0)(31, 7)$
$(73, -30)$	$(2, 0)(29, 10)$
$(13, 4)$	$(71, -21)$

все дивизоры  $A$ , для которых дивизор  $(3, 0)$   $A$  главный, являются неглавными. Повторным применением этого приема ко всем главным дивизорам из табл. 5.2.2 мы обнаружим, что неглавные дивизоры, входящие в этот список, уже перечислены ранее, поскольку все они оказываются сопряженными дивизорам из табл. 5.2.3. И вообще, любые дальнейшие попытки показали бы, что для данного неглавного дивизора  $B$  каждый дивизор  $A$ , для которого дивизор  $BA$  является главным, либо совпадает с некоторым дивизором из табл. 5.2.3, либо сопряжен с таким дивизором.

Другим способом ту же мысль можно высказать так: если  $B$  — любой дивизор и в табл. 5.2.3 найдется такой дивизор  $A$ , при котором  $BA$  есть главный дивизор, то  $BA$  является главным дивизором и при *всех*  $A$  из табл. 5.2.3. Как только это явление обнаружено, легко доказать его в общем виде. Пусть  $A$  и  $A'$  взяты из табл. 5.2.3, и пусть  $BA$  — главный дивизор. Тогда все дивизоры  $(2, 0)$   $A$ ,  $(2, 0)$   $A'$  и  $BA$  являются главными. Пусть они являются дивизорами элементов  $a + b\theta_0$ ,  $c + d\theta_0$  и  $e + f\theta_0$  соответственно. Тогда, по основной теореме,  $a + b\theta_0$  делит  $(c + d\theta_0) \times (e + f\theta_0)$  и частное имеет дивизор  $BA'$ . Частное инвариантно при  $\alpha \mapsto \alpha^4$  и, следовательно, имеет вид  $g + h\theta_0$ . Таким образом,  $BA'$  есть главный дивизор, что и требовалось установить. Все это

показывает, что все дивизоры из таблицы *эквивалентны* в следующем смысле.

**Определение.** Два дивизора <sup>1)</sup>  $A$  и  $A'$  называются *эквивалентными* (обозначается  $A \sim A'$ ), если для всех дивизоров  $B$  дивизор  $AB$  тогда и только тогда является главным, когда главным является дивизор  $A'B$ . Иными словами, в любом дивизоре, делящемся на  $A$ , можно заменять  $A$  на  $A'$ , и новый дивизор будет главным в том и только в том случае, когда главным был первоначальный дивизор.

Из самого определения очевидно, что это отношение эквивалентности рефлексивно, симметрично и транзитивно (если  $A$  можно заменить на  $A'$ , а  $A'$  можно заменить на  $A''$ , то  $A$  можно заменить на  $A''$ ) и согласовано с умножением (если  $A$  можно заменить на  $A'$ , то  $AC$  можно заменить на  $A'C$ ).

Выше было показано, что если существует один такой дивизор  $C$ , что оба дивизора  $CA$  и  $CA'$  главные, то  $A \sim A'$ . (В доказательстве мы взяли  $C = (2, 0)$ .) Следовательно, эквивалентны друг другу не только все дивизоры из табл. 5.2.3 ( $C = (2, 0)$ ), но и все их сопряженные ( $C = (2, 1)$ ), а также все главные дивизоры ( $C = I$ ). Небольшое экспериментальное исследование показывает, что каждый дивизор вида  $(p_1, u_1)(p_2, u_2) \dots (p_s, u_s)$ , по всей вероятности, лежит в одном из этих трех классов эквивалентности. Сейчас мы убедимся, что верно не только это, но и то, что при помощи простого вычисления можно установить для данного дивизора такого вида, какому именно из трех классов он принадлежит. Поскольку первоначальная задача заключалась в том, чтобы определить, когда данный дивизор указанного вида является главным, т. е. когда он эквивалентен дивизору  $I$ , то это даст нам даже больше чем решение первоначальной задачи.

Ввиду того что отношение эквивалентности дивизоров согласовано с их умножением, мы можем упростить вычисление класса произведения  $AB$  двух дивизоров, заменяя  $A$  или  $B$  или оба сомножителя эквивалентными дивизорами. Например, если  $A$  и  $B$  оба взяты из табл. 5.2.3, то оба они эквивалентны дивизору  $(3, 0)$ , а их произведение эквивалентно дивизору  $(3, 0)^2$ , который лежит в классе эквивалентности сопряженных к дивизорам из этой таблицы. Придадим этому более общую форму. Дивизор  $(3, 0)$  лежит в классе табл. 5.2.3, дивизор  $(3, 0)^2$  — в классе сопряженных к ним и, наконец,  $(3, 0)^3$  — главный дивизор; значит, если дивизоры  $A$  и  $B$  оба лежат в объединении упомянутых трех классов, то как  $A$ , так и  $B$  эквивалентны степеням дивизора  $(3, 0)$

<sup>1)</sup> В наших рассуждениях имеются в виду дивизоры, представимые в виде  $(\alpha - 1)^{11j} (p'_1)(p'_2) \dots (p'_r) (p_1, u_1)(p_2, u_2) \dots (p_s, u_s)$ , которые, следовательно, могут быть дивизорами круговых целых вида  $a + b\theta_0$ .

и, поскольку  $(3, 0)^3$  — главный дивизор, произведение  $AB$  обязано лежать в одном из этих трех классов. Более того, если классы дивизоров  $A$  и  $B$  известны, то класс дивизора  $AB$  находится простым сложением показателей по модулю 3.

Таким образом, для доказательства того, что каждое произведение дивизоров вида  $(p, u)$  принадлежит одному из трех классов, достаточно показать, что любой дивизор  $(p, u)$  лежит в одном из этих классов. В пределах наших таблиц это проверить нетрудно. Правда, дивизоры  $(2, 0)$  и  $(2, 1)$  не попали ни в одну из них, но это произошло лишь потому, что при составлении табл. 5.2.3 мы проглядели, что дивизор  $(2, 0)$   $(2, 1)$  главный. В действительности же  $(2, 1) \sim (3, 0)$ ,  $(2, 0) \sim (3, 0)^2$ . Далее, в порядке возрастания  $p$  получаем:  $(3, 0) \sim (3, 0)$ ,  $(13, 4) \sim (3, 0)$ ,  $(31, -8) \sim (3, 0)$ ,  $(41, 15) \sim (3, 0)$ ,  $(47, 13) \sim (3, 0)$ ,  $(59, 26) \sim I$ ,  $(71, -21) \sim (3, 0)$ ,  $(73, -30) \sim (3, 0)$ ,  $(101, 24) \sim I$ . Разумеется, любой дивизор, сопряженный тем, которые эквивалентны дивизору  $(3, 0)$ , эквивалентен дивизору  $(3, -1) \sim (3, 0)^2$ .

Рассмотрим теперь произвольный дивизор вида  $(p, u)$ . Он делит  $\theta_0 - u$ . Так как он делит также число  $p$ , мы можем редуцировать число  $u$  по модулю  $p$ , заменив его наименьшим по абсолютной величине вычетом, т. е. так, чтобы  $|u| \leq p/2$ . Тогда целое число  $(\theta_0 - u)(\theta_1 - u) = u^2 + u + 6$  положительно (его 11-я степень является нормой) и не превосходит числа  $\frac{1}{4}p^2 + \frac{1}{2}p + 6$ . При достаточно больших  $p$  это число меньше  $p^2$ . Именно, оно меньше  $p^2$  для всех  $p$ , кроме 2 и 3. Дивизор  $(p, u)$  и его сопряженный оба делят число  $(\theta_0 - u)(\theta_1 - u)$ , поэтому  $(\theta_0 - u)(\theta_1 - u) = rk$ , где  $k < p$  (случаи  $p = 2$  и  $3$  исключены). Дивизор элемента  $\theta_0 - u$  имеет вид  $(\alpha - 1)^{11j} (p'_1) (p'_2) \dots (p'_r) (p, u) (p_1, u_1) \times \times (p_2, u_2) \dots (p_s, u_s)$ . Более того,  $r = 0$ , поскольку из  $r > 0$  вытекало бы, что  $p'_1$  делит  $\theta_0 - u$ , тогда как в действительности ни одно целое число, большее единицы, не делит  $\theta_0 - u$ . Итак,  $rk = 23^j p p_1 p_2 \dots p_s$ . С другой стороны,  $(p, -1 - u) \sim (\alpha - 1)^{11j} (p_1, u_1) (p_2, u_2) \dots (p_s, u_s)$ , поскольку оба эти дивизора становятся главными после домножения их на  $(p, u)$ . Так как  $(\alpha - 1)^{11j} \sim I$  (это дивизор числа  $(1 + 2\theta_1)^j$ ), то это дает  $(p, u) \sim (p_1, -1 - u_1) (p_2, -1 - u_2) \dots (p_s, -1 - u_s)$ . Иными словами, любой дивизор вида  $(p, u)$  при  $p > 3$  эквивалентен произведению дивизоров такого же вида, но соответствующих простым числам, строго меньшим первоначального  $p$ . Если некоторые из появившихся простых чисел оказались больше 3, то эта операция повторяется до приведения к эквивалентности окончательного вида:  $(p, u) \sim (p''_1, u''_1) (p''_2, u''_2) \dots (p''_t, u''_t)$ , где все  $p''_j$  равны 2 или 3. Это доказывает, что  $(p, u)$  эквивалентен либо  $(3, 0)$ , либо  $(3, 0)^2$ , либо  $(3, 0)^3 \sim I$ .

Итак, если эквивалентность дивизоров вида  $(\alpha - 1)^{11j} (p'_1) \times \times (p'_2) \dots (p'_r) (p_1, u_1) (p_2, u_2) \dots (p_s, u_s)$  определена, как вы-

ше, то каждый такой дивизор эквивалентен одному и только одному из трех дивизоров  $I$ ,  $(3, 0)$  или  $(3, 0)^2$ . Более того, выше приведена явная процедура, позволяющая определить, какая из трех возможных эквивалентностей имеет место. Наконец, получено решение сформулированной ранее задачи: *данный дивизор является главным тогда и только тогда, когда он имеет указанный вид и эквивалентен  $I$ .*

## Упражнение

1. Для каждого из случаев  $\lambda = 31, 39, 43$  найдите формулу для  $(a + b\theta_0) \times \times (a + b\theta_1)$ , постройте таблицы, аналогичные таблицам 5.2.1 и 5.2.2, и найдите такую систему дивизоров, подобную тройке  $I, (3, 0), (3, 0)^2$  для  $\lambda = 23$ , чтобы (1) каждый дивизор был бы эквивалентен одному из дивизоров этой системы и (2) никакие два дивизора системы не были эквивалентны между собой.

## 5.3. Число классов

В предыдущем параграфе даны определения главного дивизора и эквивалентных дивизоров для дивизоров чисел вида  $a + b\theta_0 + + c\theta_1$  при  $\lambda = 23$ . Общие определения получаются из этого частного случая очевидным образом. Дивизор (для некоторого фиксированного  $\lambda$ ) называется *главным*<sup>1)</sup>, если существует круговое целое, дивизором которого он является. Два дивизора  $A$  и  $B$  называются *эквивалентными* (обозначается  $A \sim B$ ), если дивизор  $AC$  является главным тогда и только тогда, когда дивизор  $BC$  главный. Иными словами,  $A \sim B$  означает, что  $A$  можно заменять как сомножитель на  $B$  в любом дивизоре, делящемся на  $A$ , и новый дивизор будет главным в том и только в том случае, когда первоначальный дивизор был главным. Легко доказать следующие свойства, вытекающие из этих определений (упр. 1):

- (1) Если  $A$  и  $B$  оба главные, то таким же будет и  $AB$ .
- (2) Если  $A$  и  $B$  — такие дивизоры, что  $A$  и  $AB$  оба главные, то  $B$  — главный дивизор.
- (3) Дивизор  $A$  тогда и только тогда главный, когда  $A \sim I$ , где  $I$  — пустой дивизор, т. е. дивизор числа 1.
- (4)  $A \sim B$  тогда и только тогда, когда существует такой дивизор  $C$ , что дивизоры  $AC$  и  $BC$  оба главные. (Это как раз тот способ, которым определял эквивалентность дивизоров Куммер.)
- (5) Отношение эквивалентности дивизоров рефлексивно, симметрично и транзитивно:  $A \sim A$ ; если  $A \sim B$ , то  $B \sim A$ ; если  $A \sim B$  и  $B \sim C$ , то  $A \sim C$ .

---

<sup>1)</sup> Происхождение этого странного названия выясняется в § 8.5. Было бы точнее, но длиннее называть такой дивизор дивизором «из главного класса», считая, что классы отвечают введенному здесь отношению эквивалентности, а главный класс — это класс дивизора  $I$ .

(6) Умножение дивизоров согласовано с отношением эквивалентности: из  $A \sim B$  следует  $AC \sim BC$  для всех дивизоров  $C$ .

(7) Для любого данного дивизора  $A$  имеется такой дивизор  $B$ , что  $AB \sim I$ .

(8)  $A \sim B$  тогда и только тогда, когда существуют такие главные дивизоры  $M$  и  $N$ , что  $AM \sim BN$ . (Это является точным аналогом определения сравнения  $a \equiv b \pmod{k}$ , данного в приложении, § А.1. Именно, существуют такие целые положительные  $m$  и  $n$ , делящиеся на  $k$ , что  $a + m = b + n$ .)

Куммер доказал, что во всех случаях (т. е. для всех  $\lambda > 2$ ) можно найти *конечное число* таких дивизоров  $A_1, A_2, \dots, A_k$ , что каждый дивизор эквивалентен одному из  $A_i$  (точно так же, как в предыдущем параграфе для круговых целых  $a + b\theta_0 + c\theta_1$  в случае  $\lambda = 23$  каждый дивизор эквивалентен одному из трех дивизоров:  $I$ ,  $(3, 0)$  или  $(3, 0)^2$ ). Доказательство этого важного факта дано в конце этого параграфа.

*Системой представителей* дивизоров мы будем называть систему дивизоров  $A_1, A_2, \dots, A_k$ , обладающую сформулированным выше свойством, что каждый дивизор эквивалентен одному из  $A_i$ , и дополнительным свойством, что никакие два дивизора из этой системы не эквивалентны между собой. Такая система представителей делает возможной *классификацию* дивизоров. Каждый дивизор эквивалентен одному и только одному из  $A_i$ , и два дивизора тогда и только тогда принадлежат одному и тому же *классу эквивалентности*, т. е. эквивалентны друг другу, когда они эквивалентны одному и тому же  $A_i$ . Таким образом, число дивизоров в системе представителей есть число различных классов эквивалентности. Это число называется *числом классов*.

Казалось бы, для того чтобы найти систему представителей и тем самым определить число классов, нужно только взять систему  $A_1, A_2, \dots, A_k$ , существование которой обеспечено теоремой Куммера, и исключить повторения, т. е. если  $A_1, A_2, \dots, A_k$  еще не является системой представителей, то  $A_i \sim A_j$  для некоторых  $i$  и  $j$ , так что один дивизор из этой пары можно исключить, не нарушая свойства, что любой дивизор эквивалентен одному из дивизоров системы; продолжение этого процесса должно в конце концов привести к системе представителей. Однако это «построение» иллюзорно, поскольку оно включает в себя решение проблемы выяснения, эквивалентны или нет два данных дивизора, т. е. проблемы, требующей добавочных технических приемов и возвращающей нас к основной проблеме, из которой в первую очередь и возникла вся теория эквивалентности.

В том-то и дело, что теоремы Куммера недостаточно для конструктивного доказательства существования системы представителей и что, как говорит Куммер в последней части своего перво-



начального изложения 1847 г. теории идеальной факторизации, подсчет числа классов требует «принципов, совершенно отличных от тех, которые содержатся в настоящей работе». Эти новые принципы и определение числа классов, опубликованные Куммером позже в 1847 г., составляют предмет гл. 6. Все, что будет использовано в настоящей главе о понятии числа классов, — это его *значение*: если сказано, что число классов для данного  $\lambda$  есть  $h$ , то это означает, что можно построить систему из  $h$  дивизоров  $A_1, A_2, \dots, A_h$  (для этого  $\lambda$ ) с тем свойством, что каждый дивизор эквивалентен одному и только одному из  $A_i$  ( $i = 1, 2, \dots, h$ ).

Остальная часть этого параграфа посвящена доказательству теоремы Куммера о том, что существует конечная система  $A_1, A_2, \dots, A_h$  дивизоров, обладающая тем свойством, что каждый дивизор эквивалентен одному из  $A_i$ . Доказательство сходно с данным в предыдущем параграфе доказательством того, что каждый простой дивизор эквивалентен произведению простых дивизоров с меньшими нормами. Точнее, мы докажем, что для любого данного дивизора  $A$  (в предыдущем параграфе рассматривались лишь дивизоры  $(p, u)$ ) имеется круговое целое  $(\theta_0 - u$  в предыдущем параграфе), которое делится на  $A$  и норма которого, деленная на норму дивизора  $A$ , меньше некоторой постоянной  $K$ , не зависящей от  $A$ , т. е. имеется такой дивизор  $B$  с нормой, меньшей  $K$ , что дивизор  $AB$  главный. Число дивизоров с нормой, меньшей  $K$ , конечно. Значит, найдется такая конечная система  $B_1, B_2, \dots, B_k$ , что для каждого данного  $A$  дивизор  $AB_i$  главный при некотором  $i$ . Для каждого  $B_i$  отыщем такой дивизор  $A_i$ , что  $A_i B_i$  главный. Тогда каждый данный дивизор  $A$  эквивалентен одному из  $A_i$ , и система  $A_1, A_2, \dots, A_k$  дивизоров с требуемым свойством будет найдена.

Итак, нам надо показать, что имеется постоянная  $K$  с тем свойством, что если  $A$  — любой данный дивизор и  $n$  — его норма, то имеется круговое целое, делящееся на  $A$ , норма которого меньше  $Kn$ . Это наводит на мысль поискать круговое целое, которое делится на  $A$  и имеет настолько малую норму, насколько это возможно. А это очень просто сделать на основании теоремы из § 4.14 о том, что число не сравнимых по модулю  $A$  круговых целых есть  $NA$ , поскольку эта теорема показывает, что *любая система из более чем  $n$  различных круговых целых должна содержать два таких, разность между которыми делится на  $A$* . Так как величина нормы связана с величиной коэффициентов кругового целого, естественный путь построения кругового целого, делящегося на  $A$  и имеющего малую норму, состоит в том, чтобы взять систему из более чем  $n$  круговых целых, имеющих малые коэффициенты. Это подсказывает мысль об установлении взаимосвязи между величиной коэффициентов и величиной нормы, которая может быть получена следующим образом.



Пусть  $g(\alpha) = a_0 + a_1\alpha + \dots + a_{\lambda-1}\alpha^{\lambda-1}$ . Тогда

$$Ng(\alpha) = g(\alpha)g(\alpha^2)\dots g(\alpha^{\lambda-1}) = [g(\alpha)g(\alpha^{-1})][g(\alpha^2)g(\alpha^{-2})]\dots,$$

и каждый из  $(\lambda - 1)/2$  членов этого произведения можно рассматривать как квадрат модуля комплексного числа  $g(\alpha^j)$ . В таком случае ясно, что каждый из этих  $(\lambda - 1)/2$  членов не превосходит квадрата числа  $|a_0| + |a_1| + \dots + |a_{\lambda-1}|$ . Следовательно, если все  $a_i$  удовлетворяют неравенству  $|a_i| \leq c$ , то

$$Ng(\alpha) \leq (\lambda^2 c^2)^{(\lambda-1)/2} = \lambda^{\lambda-1} c^{\lambda-1}.$$

Система из всех тех  $g(\alpha)$ , для которых  $a_0 = 0$  и  $0 \leq a_i \leq c$  при  $i > 0$ , содержит более чем  $n$  элементов, при условии что  $(c + 1)^{\lambda-1} > n$ . Значит, разность некоторых двух из этих элементов делится на  $A$  и имеет норму самое большее  $\lambda^{\lambda-1} c^{\lambda-1}$ . Если  $c$  — наименьшее число, при котором  $(c + 1)^{\lambda-1} > n$ , то, конечно,  $c^{\lambda-1} \leq n$ , и круговое целое, делящееся на  $A$  и имеющее норму, не превосходящую  $\lambda^{\lambda-1} n$ , найдено. Это доказывает теорему и дает значение  $\lambda^{\lambda-1}$  величине  $K$ . (Доказательство Куммера основывалось на более тонкой оценке нормы  $Ng(\alpha)$ : оно дает для  $K$  лучшее значение  $(\lambda - 1)^{(\lambda-1)/2}$ . См. упр. 3.)

## Упражнения

1. Выведите свойства (1) — (8) из определений главного дивизора и эквивалентности дивизоров.

2. Докажите, что для данного  $\lambda$  единственность разложения имеет место тогда и только тогда, когда соответствующее число классов есть 1.

3. Куммер оценил норму  $Ng(\alpha)$ , установив тождество  $g(\alpha)g(\alpha^{-1}) + g(\alpha^2)g(\alpha^{-2}) + \dots + g(\alpha^{\lambda-1})g(\alpha^{-\lambda+1}) = \lambda(a_1^2 + a_2^2 + \dots + a_{\lambda-1}^2) - (a_1 + a_2 + \dots + a_{\lambda-1})^2$  (где  $a_0 = 0$ ) и применив теорему о том, что среднее геометрическое  $\sqrt[n]{c_1 c_2 \dots c_n}$  множества положительных чисел всегда не больше их среднего арифметического  $n^{-1}(c_1 + c_2 + \dots + c_n)$ . Примените это для нахождения значения  $K = (\lambda^{\lambda-1})^{1/2}$ . Заметим, что оба эти доказательства основаны на интерпретации кругового целого  $g(\alpha)$  как комплексного числа.

## 5.4. Два условия Куммера

Выше мы уже несколько раз отмечали, что центральной идеей в доказательствах Последней теоремы Ферма является идея доказательства следующего утверждения: если  $u$  и  $v$  таковы, что их произведение есть  $\lambda$ -я степень,  $uv = w^\lambda$  (где  $\lambda$  — простой показатель, для которого доказывается Последняя теорема Ферма  $x^\lambda + y^\lambda \neq z^\lambda$ ), и  $u$  и  $v$  взаимно просты, то  $u$  и  $v$  должны быть оба  $\lambda$ -ми степенями. Этот вывод был бы верен, если бы имела место единственность разложения в строгом смысле. Однако даже если  $\lambda$  таково, что для соответствующих ему круговых целых выполнена

единственность разложения (т. е. соответствующее число классов равно 1), этот вывод все же неверен, поскольку «единственность» обычно означает «единственность с точностью до сомножителей, являющихся единицами». Таким образом, даже в простейшем случае такой вывод не обоснован, пока на  $u$  и  $v$  не наложены, дополнительные условия. Какие же это условия?

Заметим, во-первых, что единственность разложения в строгом смысле *имеет место для дивизоров* и что из  $uv = w^\lambda$  действительно вытекает, что если  $u$  и  $v$  не имеют общих идеальных простых делителей, то каждый из их дивизоров является  $\lambda$ -й степенью. Таким образом, если  $A$  и  $B$  — дивизоры чисел  $u$  и  $v$  соответственно,  $uv = w^\lambda$  и  $A$  и  $B$  не имеют общих делителей, то существуют такие дивизоры  $C$  и  $D$ , что  $A = C^\lambda$  и  $B = D^\lambda$ . Так как естественным определением свойства « $u$  и  $v$  взаимно просты» является формулировка «никакой идеальной простой делитель не делит  $u$  и  $v$  одновременно», то поставленный выше вопрос сводится к следующему. Пусть  $u$  — круговое целое, дивизор которого  $A$  является  $\lambda$ -й степенью другого дивизора:  $A = C^\lambda$ . При каких дополнительных условиях на  $\lambda$  и  $u$  можно заключить, что само  $u$  есть  $\lambda$ -я степень?

Естественно, это приводит к вопросу, является ли  $C$  главным, т. е. следует ли из  $C^\lambda = A \sim I$  (поскольку  $A$  — дивизор элемента  $u$ ) эквивалентность  $C \sim I$ . Куммер нашел очень естественное условие на  $\lambda$ , при котором эта импликация выполняется без всяких предположений относительно  $u$ . Это условие основывается на простом наблюдении, что *если  $C$  — любой дивизор, а  $h$  — число классов, соответствующее  $\lambda$ , то  $C^h \sim I$* . Это утверждение является, очевидно, обобщением <sup>1)</sup> теоремы Ферма и легко доказывается. То что число классов равно  $h$ , означает, что имеется система представителей  $A_1, A_2, \dots, A_h$ , состоящая из  $h$  элементов. Каждая из степеней  $C, C^2, C^3, \dots$  дивизора  $C$  эквивалентна одному и только одному из  $A_i$ . Очевидно, что некоторые различные степени дивизора  $C$  должны оказаться эквивалентными одному и тому же  $A_i$  и, следовательно, друг другу, например  $C^j \sim C^{j+k}$ . Тогда  $C^k \sim I$ , т. е. некоторая степень дивизора  $C$  эквивалентна дивизору  $I$ . Таким образом, мы можем попробовать (при помощи системы представителей) все меньшие степени дивизора  $C$  подряд и найти *первую* из них, которая эквивалентна дивизору  $I$ , скажем  $C^d \sim I$ . Тогда  $I, C, C^2, \dots, C^{d-1}$  попарно не эквивалентны ( $C^j \sim C^{j+k}$  дает  $C^k \sim I$ ) и, следовательно, эквивалентны некоторым  $d$  дивизорам из  $A_i$ . Если этим исчерпываются все  $A_i$ , то  $d = h$ . В противном случае имеется такое  $A_i$ , обозначим его  $B$ , которого нет в множестве этих  $d$  дивизоров. Тогда последователь-

<sup>1)</sup> Оба эти утверждения обобщает такая теорема: если  $H$  — подгруппа конечной группы  $G$ , то порядок группы  $H$  делит порядок группы  $G$ .

ность  $B, BC, BC^2, \dots, BC^{d-1}$  дает еще  $d$  дивизоров, которые не эквивалентны друг другу и дивизорам из первого набора. Это дает другое подмножество из  $d$  дивизоров в системе представителей. Продолжение этого процесса производит разбиение множества всех элементов системы представителей на непересекающиеся подмножества, каждое из которых содержит  $d$  элементов. Значит,  $d \mid h$  и из  $C^d \sim I$  вытекает  $C^h \sim I$ , что и требовалось доказать.

Если вдобавок  $C^\lambda \sim I$ , то  $C \sim I$ , кроме случая  $\lambda \mid h$ . Это вытекает из следующего замечания. Число  $\lambda$  — простое, поэтому если  $h$  не делится на  $\lambda$ , то  $mh = n\lambda + 1$  для подходящих  $m$  и  $n$ , откуда  $I \sim (C^h)^m = C^{mh} = C^{n\lambda+1} = (C^\lambda)^n C \sim I \cdot C \sim C$ . Следовательно, требуемая импликация  $C^\lambda \sim I \Rightarrow C \sim I$  верна, если только  $\lambda$  удовлетворяет условию Куммера:

(А) Показатель  $\lambda$  не делит соответствующее число классов  $h$ .

Если  $u$  — круговое целое, дивизор  $A$  которого является  $\lambda$ -й степенью, т. е.  $A = C^\lambda$ , и если условие (А) выполнено, то  $C \sim I$  (поскольку  $C^\lambda$  есть дивизор элемента  $u$ , откуда следует  $C^\lambda \sim I$ ); пусть, скажем,  $C$  есть дивизор кругового целого  $x$ . Тогда  $u$  и  $x^\lambda$  имеют один и тот же дивизор и отсюда по основной теореме следует, что  $u = ex^\lambda$ , где  $e$  — круговая единица, т. е. круговое целое, являющееся единицей. Короче, условие (А) гарантирует, что каждое круговое целое  $u$ , дивизор которого есть  $\lambda$ -я степень, имеет вид  $u = ex^\lambda$ , где  $e$  и  $x$  — круговые целые, причем  $e$  — единица. Задача заключается в том, чтобы найти еще условие, при котором имеет место более сильное утверждение  $u = x^\lambda$ .

Центральной идеей доказательства Дирихле для случая  $\lambda = 5$  (см. § 3.3) было, как говорил он сам, нахождение *дополнительного условия*, при котором из того, что  $P^2 + 5Q^2$  — пятая степень и  $P$  и  $Q$  взаимно просты, вытекает

$$P + Q\sqrt{5} = (A + B\sqrt{5})^5.$$

Без дополнительных требований к  $P$  и  $Q$  это утверждение *не имеет места*. Дополнительное условие, которое ввел Дирихле, извлечено из того, что в разложении бинома  $(A + B\sqrt{5})^5$  все слагаемые, кроме первого, содержат множитель 5, так что из  $P + Q\sqrt{5} = (A + B\sqrt{5})^5$  вытекает  $Q \equiv 0 \pmod{5}$ . Дирихле показал, что это *необходимое* условие в сочетании с двумя другими условиями:  $P^2 + 5Q^2$  — пятая степень и  $P, Q$  взаимно просты, — оказывается также и *достаточным*.

Легко получить соответствующее необходимое условие в случае круговых целых. В § 4.5 было отмечено, что по модулю  $\lambda$  операция возведения в  $\lambda$ -ю степень переводит сумму в сумму, т. е.  $(a + b)^\lambda \equiv a^\lambda + b^\lambda \pmod{\lambda}$ . Таким образом, из  $u = x^\lambda$

вытекает

$$\begin{aligned} u &= (a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-1}\alpha^{\lambda-1})^\lambda \equiv \\ &\equiv a_0^\lambda + a_1^\lambda + \dots + a_{\lambda-1}^\lambda = \text{целое число} \pmod{\lambda}. \end{aligned}$$

Значит, необходимым условием для  $u = x^\lambda$  является то, что  $u$  есть целое число по модулю  $\lambda$ . Следуя Дирихле, теперь естественно попытаться показать, что условие « $u$  сравнимо с целым числом по модулю  $\lambda$ » вместе с условием «дивизор элемента  $u$  является  $\lambda$ -й степенью» становится уже достаточным.

Однако это условие в том виде, как мы его сформулировали, очевидно, все же недостаточно, поскольку оно тривиальным образом выполняется, если  $u \equiv 0 \pmod{\lambda}$ . Как будет видно в следующем параграфе, это простое соображение лежит в основе различия между случаями I и II Последней теоремы Ферма. В более легком случае  $u \not\equiv 0 \pmod{\lambda}$  из условий « $u$  сравнимо с целым числом по модулю  $\lambda$ » и «дивизор элемента  $u$  является  $\lambda$ -й степенью» вытекает, при соблюдении условия (A), что  $u = ex^\lambda$  для некоторых круговых целых  $e$  и  $x$ , где  $e$  — единица. Вопрос о том, является ли  $u$   $\lambda$ -й степенью, свелся к вопросу о том, является ли  $e$   $\lambda$ -й степенью. Предположения об  $u$  гарантируют, что  $e$  сравнимо с целым числом по модулю  $\lambda$ , поскольку  $u \equiv ex^\lambda \equiv e \cdot b \pmod{\lambda}$  для некоторого целого  $b$ , причем  $b \not\equiv 0 \pmod{\lambda}$  (иначе  $u \equiv 0 \pmod{\lambda}$ ), так что, поделив сравнение  $u \equiv \text{целое число} \pmod{\lambda}$  на  $b$ , мы получим сравнение  $e \equiv \text{целое число} \pmod{\lambda}$ . Следовательно, требуемый вывод  $u = x^\lambda$  будет верен, если он верен в частном случае, когда  $u = e$  — единица. Это и есть второе условие Куммера:

(B) Показатель  $\lambda$  обладает тем свойством, что для единиц соответствующих круговых целых необходимое условие « $e$  сравнимо с целым числом по модулю  $\lambda$ » того, что  $e$  есть  $\lambda$ -я степень, оказывается также и достаточным. Короче, если  $e$  — единица, сравнимая с целым числом по модулю  $\lambda$ , то  $e = (e')^\lambda$  для некоторого кругового целого  $e'$ . (Конечно,  $e'$  — единица; ее обратный элемент есть  $(e')^{\lambda-1}e^{-1}$ .)

Куммер обнаружил, что это условие выполнено для всех тех простых  $\lambda$ , которые он испытывал, по крайней мере для тех, для которых он смог доказать условие (A). Из этих двух условий (A) и (B), когда они имеют место, вытекает следующая теорема о равенстве  $u = x^\lambda$  для круговых целых при соответствующем  $\lambda$ :

**Теорема.** *Предположим, что  $\lambda$  удовлетворяет условиям (A) и (B), и пусть задано  $u$ . Нужно узнать, является ли  $u$   $\lambda$ -й степенью. Если  $u \not\equiv 0 \pmod{\lambda}$  (случай I), то  $u$  тогда и только тогда является  $\lambda$ -й степенью, когда его дивизор является  $\lambda$ -й степенью, а само  $u$*

сравнимо с целым числом по модулю  $\lambda$ . Если  $u \equiv 0 \pmod{\lambda}$  (случай II), то  $u$  тогда и только тогда является  $\lambda$ -й степенью, когда его дивизор является  $\lambda$ -й степенью, а его частное от деления на наивысшую содержащуюся в нем степень элемента  $\alpha - 1$  сравнимо с целым числом по модулю  $\lambda$ .

Доказательство этой теоремы непосредственно следует из замечаний, которыми мотивировались условия (A) и (B). Простое число  $\lambda$  называется *регулярным*, если оно удовлетворяет условиям (A) и (B). Именно для этих простых чисел справедливо куммерово общее доказательство Последней теоремы Ферма, приводимое в следующем параграфе.

Когда Куммер впервые сформулировал условия (A) и (B), он высказал три примечательные гипотезы. Первая заключалась в том, что не все простые числа удовлетворяют этим условиям, т. е. существуют *иррегулярные* простые; вторая — что из (A) вытекает (B), так что условие (B) излишне, и третья — что регулярных простых бесконечно много. Первые две, как доказал всего через несколько месяцев сам Куммер, верны. (Доказательство приводится в гл. 6.) Однако третья представляет собой *все еще* не решенную проблему, и Куммер позже взял свои слова обратно и говорил, что не знает, существует ли бесконечно много регулярных простых чисел. (По иронии судьбы, было *доказано*, что иррегулярных простых бесконечно много.)

## Упражнения

1. Докажите теорему, приведенную в этом параграфе.

2. Докажите, что круговое целое  $u = b_0 + b_1\alpha + \dots + b_{\lambda-1}\alpha^{\lambda-1}$  тогда и только тогда сравнимо по модулю  $\lambda$  с целым числом, когда  $b_1 \equiv b_2 \equiv \dots \equiv b_{\lambda-1} \pmod{\lambda}$ .

## 5.5. Доказательство для регулярных простых

По многим книгам, посвященным Последней теореме Ферма, создается впечатление, что ее доказательство было бы легким, если бы имела место единственность разложения на простые для круговых целых. О том, до какой степени ошибочно это впечатление, можно судить по доказательству, которое сейчас последует. Доказательство ничуть не стало бы легче, если бы куммерово предположение (A) было заменено более жестким предположением единственности разложения. И даже если используется еще свойство (B) (в гл. 6 будет показано, что (B) на самом деле является тонким следствием свойства (A)), нужно еще много изобретательности, чтобы завершить доказательство.

В доказательстве Куммера существенно используется одно частное свойство единиц, совсем не очевидное, но в своей основе

совершенно элементарное и наверняка известное в 1847 г. Куммеру, Кронекеру, Дирихле и другим, интересовавшимся структурой единиц круговых целых. Речь идет о следующем свойстве: если  $e$  — круговое целое, являющееся единицей, а  $\bar{e}$  — его *комплексно сопряженное* (получаемое из  $e$  заменой в нем  $\alpha$  на  $\alpha^{-1}$ ), то  $e/\bar{e} = \alpha^r$  для некоторого целого  $r$ . Это свойство вполне правдоподобно. Операция комплексного сопряжения, очевидно, переводит число  $e/\bar{e}$  в ему обратное. Поэтому  $e/\bar{e}$ , рассматриваемое как комплексное число, лежит на единичной окружности. А это ведет к предположению, что  $e/\bar{e}$ , возможно, имеет вид  $\alpha^r$  или, в крайнем случае,  $\pm\alpha^r$ , но доказательство не очевидно. Оно приведено в конце этого параграфа.

Первый шаг доказательства Последней теоремы Ферма для регулярных простых заключается, конечно, в том, чтобы записать уравнение  $x^\lambda + y^\lambda = z^\lambda$  в виде  $(x + y)(x + \alpha y)(x + \alpha^2 y) \dots (x + \alpha^{\lambda-1} y) = z^\lambda$ . Прежде всего нужно спросить, взаимно просты или нет сомножители в левой части. Если  $x + \alpha^j y$  и  $x + \alpha^{j+k} y$  имеют общий делитель, то этот же делитель делит как

$$(x + \alpha^{j+k} y) - (x + \alpha^j y) = \alpha^j (\alpha^k - 1) y = \text{единица} \cdot (\alpha - 1) \cdot y,$$

так и

$$(x + \alpha^{j+k} y) - \alpha^k (x + \alpha^j y) = \text{единица} \cdot (\alpha - 1) \cdot x.$$

Так как  $x$  и  $y$  — взаимно простые целые числа, они не имеют никакого — даже идеального — общего делителя, и единственным возможным общим делителем правых частей является  $\alpha - 1$ . Далее, те же самые равенства показывают, что если  $\alpha - 1$  делит один из сомножителей  $x + \alpha^j y$ , то он делит и все остальные. Таким образом, вопрос естественным образом разбивается на два обычных случая: первый, в котором  $\lambda$  делит  $z$  и, следовательно,  $\alpha - 1$  делит все сомножители выражения  $x^\lambda + y^\lambda$ , и второй, в котором  $z$  взаимно просто с  $\lambda$  и, следовательно, сомножители выражения  $x^\lambda + y^\lambda$  взаимно просты. Но  $\lambda$  нечетно, поэтому если  $x$  делится на  $\lambda$ , то уравнение можно записать в виде  $x^\lambda = z^\lambda + (-y)^\lambda$ , а если  $y$  делится на  $\lambda$ , то его можно записать в виде  $y^\lambda = z^\lambda + (-x)^\lambda$ . Следовательно, если любое из трех неизвестных делится на  $\lambda$ , то можно считать, что им является  $z$ , и случаи оказываются такими:

*Случай I:*  $x^\lambda + y^\lambda = z^\lambda$ , где  $x, y, z$  попарно взаимно просты и все взаимно просты с  $\lambda$ .

*Случай II:*  $x^\lambda + y^\lambda = z^\lambda$ , где  $x, y, z$  попарно взаимно просты и  $\lambda \mid z$ .

*Доказательство случая I.* В этом случае сомножители  $x + y, x + \alpha y, \dots, x + \alpha^{\lambda-1} y$  попарно взаимно просты и их произведе-



ние есть  $\lambda$ -я степень. Следовательно, дивизор каждого сомножителя есть  $\lambda$ -я степень и на основании свойства (А) для простого числа  $\lambda$  каждый сомножитель  $x + \alpha^j y$  есть единица, умноженная на  $\lambda$ -ю степень. Куммер в своем доказательстве разбирает только случай  $j = 1$ , т. е. пользуется лишь тем, что существуют единица  $e$  и круговое целое  $t$ , для которых  $x + \alpha y = et^\lambda$ . Замена  $\alpha$  на  $\alpha^{-1}$  приводит это равенство к виду  $x + \alpha^{-1}y = \bar{e}\bar{t}^\lambda$ . Далее,  $e/\bar{e} = \alpha^r$  на основании приведенного выше свойства единиц, и  $t^\lambda \equiv C \equiv \bar{C} \equiv \bar{t}^\lambda \pmod{\lambda}$ , поскольку каждая  $\lambda$ -я степень сравнима по модулю  $\lambda$  с целым числом, а целые числа не меняются при замене  $\alpha \mapsto \alpha^{-1}$ . Таким образом,  $x + \alpha^{-1}y = \alpha^{-r}\bar{e}t^\lambda \equiv \alpha^{-r}et^\lambda = \alpha^{-r}(x + \alpha y) \pmod{\lambda}$ . Заключительная часть <sup>1)</sup> доказательства состоит в следующем. Запишем члены сравнения

$$\alpha^r (x + \alpha^{-1}y) \equiv x + \alpha y \pmod{\lambda}$$

через произведения целых чисел и степеней элемента  $\alpha - 1$  и посмотрим, какие условия налагает это сравнение на целые числа  $x$ ,  $y$  и  $r$ . Заметим сразу, что  $r$  определено лишь по модулю  $\lambda$  и что  $r \equiv 0 \pmod{\lambda}$  невозможно, поскольку это давало бы

$$x + \alpha^{-1}y \equiv x + \alpha y \pmod{\lambda}, \quad 0 \equiv (\alpha^2 - 1)y \pmod{(\alpha - 1)^{\lambda-1}},$$

откуда вытекало бы, что  $\alpha - 1$  делит  $y$ , вопреки предположению. Значит, мы можем предположить, что  $0 < r < \lambda$ . Сравнение тогда может быть записано в виде

$$\alpha^{r-1}(\alpha x + y) \equiv x + \alpha y \pmod{\lambda},$$

$$[1 + (\alpha - 1)]^{r-1}[x + y + x(\alpha - 1)] \equiv x + y + y(\alpha - 1) \pmod{(\alpha - 1)^{\lambda-1}}.$$

Далее, из сравнения вида  $a_0 + a_1(\alpha - 1) + a_2(\alpha - 1)^2 + \dots + a_{\lambda-2}(\alpha - 1)^{\lambda-2} \equiv 0 \pmod{(\alpha - 1)^{\lambda-1}}$  легко выводится (упр. 1), что  $a_0 \equiv 0$ ,  $a_1 \equiv 0$ ,  $\dots$ ,  $a_{\lambda-2} \equiv 0 \pmod{\lambda}$ . Следовательно, в нашем сравнении коэффициенты при одинаковых степенях элемента  $(\alpha - 1)$  должны быть сравнимы по модулю  $\lambda$ , при условии что показатели этих степеней меньше  $\lambda - 1$ . При  $1 < r < \lambda - 1$  наше сравнение невозможно, поскольку слагаемое высшей степени слева есть  $x(\alpha - 1)^r$ , где  $2 \leq r \leq \lambda - 2$ , а это дало бы  $x \equiv 0 \pmod{\lambda}$  вопреки предположению. Если  $r = \lambda - 1$ , то предпоследнее слагаемое слева равно

$$\begin{aligned} (\alpha - 1)^{r-1}(x + y) + (r - 1)(\alpha - 1)^{r-2}x(\alpha - 1) = \\ = [x + y + (\lambda - 2)x](\alpha - 1)^{\lambda-2}, \end{aligned}$$

---

<sup>1)</sup> Эта часть доказательства несколько расширена. Куммер просто пишет сравнение в виде  $(1 - \alpha^r)x + (\alpha - \alpha^{r-1})y \equiv 0 \pmod{\lambda}$  и заключает, что  $r \equiv 1$ ,  $x \equiv y \pmod{\lambda}$ . Возможно, он пользовался более простыми рассуждениями.

что дает  $-x + y \equiv 0 \pmod{\lambda}$ ,  $x \equiv y \pmod{\lambda}$ . (Исследование других слагаемых без труда показывает, что случай  $r = \lambda - 1$  также невозможен, но для получения противоречия достаточно заключения  $x \equiv y \pmod{\lambda}$ .) Если  $r = 1$ , то непосредственно получается то же самое утверждение  $x \equiv y \pmod{\lambda}$ .

Заметим, что случай I симметричен относительно всех трех переменных. Поэтому естественно записать в этом случае уравнение в виде  $x^\lambda + y^\lambda + z^\lambda = 0$ . Нами доказано, что из этого уравнения при  $x \not\equiv 0$ ,  $y \not\equiv 0$ ,  $z \not\equiv 0 \pmod{\lambda}$  вытекает  $x \equiv y \pmod{\lambda}$ . По симметрии вдобавок получаем  $x \equiv z$ ,  $y \equiv z \pmod{\lambda}$ . Но, по теореме Ферма,  $x^\lambda \equiv x$ ,  $y^\lambda \equiv y$ ,  $z^\lambda \equiv z \pmod{\lambda}$ . Отсюда  $0 = x^\lambda + y^\lambda + z^\lambda \equiv 3x \pmod{\lambda}$ . Так как  $x \not\equiv 0 \pmod{\lambda}$ , отсюда следует  $3 \equiv 0 \pmod{\lambda}$ , а значит,  $\lambda = 3$ . Таким образом, при  $\lambda \neq 3$  случай I невозможен. Так как невозможность случая I при  $\lambda = 3$  была уже доказана (скажем, на основании несложной теоремы из § 3.2 с учетом того, что  $2 \cdot 3 + 1 = 7$  есть простое число), этим завершается доказательство невозможности случая I для регулярных простых чисел. (На самом деле понадобилось лишь свойство (A) регулярных простых чисел.)

*Доказательство случая II.* В этом случае все сомножители выражения  $x^\lambda + y^\lambda$  делятся на  $\alpha - 1$  и частные взаимно просты. Так как произведение частных есть  $z^\lambda (\alpha - 1)^{-\lambda}$ , то произведение есть  $\lambda$ -я степень, а из свойства (A) вытекает, что  $(\alpha - 1)^{-1} (x + \alpha^j y) = e_j t_j^\lambda$  для некоторых круговых целых  $e_j$ ,  $t_j$ , причем  $e_j$  — единица. Кроме того, элементы  $t_j$  попарно взаимно просты. Особый простой элемент  $\alpha - 1$  делит не более одного из  $t_j$ , а точнее, он делит  $t_0$ , поскольку из того, что  $\alpha - 1$  делит  $x + y$ , а  $x$  и  $y$  — целые числа, вытекает, что на самом деле  $(\alpha - 1)^{\lambda-1}$  делит  $x + y$ . Пусть  $t_0 = (\alpha - 1)^k w$ , где  $w$  не делится на  $\alpha - 1$ . Тогда  $k \geq 1$ . Из  $\lambda$  равенств, полученных ранее, в частности, имеем

$$\begin{aligned} x + \alpha^{-1}y &= (\alpha - 1) e_{-1} t_{-1}^\lambda, \\ x + y &= (\alpha - 1) e_0 (\alpha - 1)^{k\lambda} w^\lambda, \\ x + \alpha y &= (\alpha - 1) e_1 t_1^\lambda. \end{aligned}$$

Используем эти 3 равенства, чтобы исключить два неизвестных  $x$  и  $y$ ; это дает

$$\begin{aligned} (\alpha - 1) y &= (\alpha - 1) [e_1 t_1^\lambda - e_0 (\alpha - 1)^{k\lambda} w^\lambda], \\ \alpha^{-1} (\alpha - 1) y &= (\alpha - 1) [e_0 (\alpha - 1)^{k\lambda} w^\lambda - e_{-1} t_{-1}^\lambda], \end{aligned}$$

а затем

$$0 = e_1 t_1^\lambda - e_0 (\alpha - 1)^{k\lambda} w^\lambda - \alpha e_0 (\alpha - 1)^{k\lambda} w^\lambda + \alpha e_{-1} t_{-1}^\lambda.$$

Так как  $\alpha + 1$  — единица (она есть частное от деления  $\alpha^2 - 1$  на  $\alpha - 1$ ), то этому равенству можно придать вид

$$E_0 (\alpha - 1)^{k\lambda} w^\lambda = t_1^\lambda + E_{-1} t_{-1}^\lambda,$$

где  $E_0, E_{-1}$  — единицы. Теперь, чтобы избавиться от множителя  $E_{-1}$ , можно воспользоваться свойством (В) простого числа  $\lambda$ , поскольку по модулю  $\lambda$  полученное равенство читается как  $0 \equiv \equiv C_1 + E_{-1} C_{-1}$ , где  $C_1, C_{-1}$  — целые числа, отличные от нуля по модулю  $\lambda$  в силу того, что  $t_1$  и  $t_{-1}$  взаимно просты с  $t_0 = (\alpha - 1)^k w$ . Значит,  $E_{-1}$  сравнимо по модулю  $\lambda$  с целым числом,  $E_{-1} = e^\lambda$  для некоторой единицы  $e$  и, наконец,  $E_0 (\alpha - 1)^{k\lambda} w^\lambda = = t_1^\lambda + (et_{-1})^k$ . Это равенство по виду очень близко к исходному уравнению  $z^\lambda = x^\lambda + y^\lambda$ , и при помощи тех же рассуждений (с небольшим лишь изменением) можно получить третье равенство того же вида.

Точнее, если мы начнем с уравнения вида

$$x^\lambda + y^\lambda = e (\alpha - 1)^{k\lambda} w^\lambda,$$

где  $e$  — единица,  $k$  — положительное целое число,  $x, y, w$  и  $\alpha - 1$  — попарно взаимно простые *круговые* целые, то можно продолжать следующим образом. (Случай II Последней теоремы Ферма получается отсюда как частный случай, когда  $x, y, w$  — *целые числа*,  $z = \lambda^m w$ ,  $k = m(\lambda - 1)$ ,  $e = [\lambda (\alpha - 1)^{-\lambda+1}]^{m\lambda}$ .) По крайней мере один из сомножителей  $x + \alpha^j y$  левой части делится на  $\alpha - 1$ , откуда, как и раньше, следует, что все сомножители делятся на  $\alpha - 1$ , а частные взаимно просты. Предыдущее доказательство того, что  $x + y$  делится на  $(\alpha - 1)^2$ , здесь не проходит, однако и в этом случае верно, что по крайней мере один из сомножителей (а значит, точно один) делится на  $(\alpha - 1)^2$ , поскольку по модулю  $(\alpha - 1)^2$  имеем

$$x \equiv a_0 + a_1 (\alpha - 1) \pmod{(\alpha - 1)^2},$$

$$y \equiv b_0 + b_1 (\alpha - 1) \pmod{(\alpha - 1)^2}$$

для некоторых целых  $a_0, a_1, b_0, b_1$  (упр. 1), откуда

$$\begin{aligned} x + \alpha^j y &\equiv [a_0 + a_1 (\alpha - 1)] + [1 + (\alpha - 1)]^j [b_0 + b_1 (\alpha - 1)] \equiv \\ &\equiv a_0 + b_0 + [a_1 + b_1 + j b_0] (\alpha - 1) \pmod{(\alpha - 1)^2}. \end{aligned}$$

Так как  $\alpha - 1$  делит  $x + \alpha^j y$  для всех  $j$ , отсюда вытекает, что  $a_0 + b_0 \equiv 0 \pmod{\lambda}$ . Кроме того, это показывает, что число  $(\alpha - 1)^2$  тогда и только тогда делит  $x + \alpha^j y$ , когда  $a_1 + b_1 + j b_0 \equiv 0 \pmod{\lambda}$ . Это условие выполняется для одного и только одного значения  $j$  по модулю  $\lambda$ , если  $b_0 \not\equiv 0 \pmod{\lambda}$ ; но  $b_0 \not\equiv 0 \pmod{\lambda}$ , так как иначе  $\alpha - 1$  делило бы  $y$ , вопреки предположению. Следовательно,  $k > 1$ . Пусть  $k = K + 1$ , где  $K$  — положительное целое число. Так как  $y$  можно заменить на  $\alpha^j y$ ,

не изменив вида первоначального уравнения, то можно предположить, что  $x + y$  и является тем сомножителем выражения  $x^\lambda + y^\lambda$ , которое делится на  $(\alpha - 1)^2$ . Тогда  $k\lambda$  сомножителей  $(\alpha - 1)$  в разложении левой части  $x^\lambda + y^\lambda$  распределены так: по одному сомножителю в каждом члене  $x + \alpha^j y$  ( $j = 1, 2, \dots, \lambda - 1$ ) и  $1 + (k - 1)\lambda = 1 + K\lambda$  сомножителей в члене  $x + y$ . Таким образом,

$$\begin{aligned}x + \alpha^{-1}y &= (\alpha - 1) e_{-1} t_{-1}^\lambda, \\x + y &= (\alpha - 1) e_0 (\alpha - 1)^{K\lambda} w^\lambda, \\x + \alpha y &= (\alpha - 1) e_1 t_1^\lambda,\end{aligned}$$

и точно такая же последовательность шагов, как и раньше, приведет нас к уравнению вида

$$X^\lambda + Y^\lambda = E (\alpha - 1)^{K\lambda} W^\lambda,$$

в котором  $X$ ,  $Y$ ,  $W$  и  $\alpha - 1$  — попарно взаимно простые круговые целые,  $E$  — единица и  $K = k - 1$ . Теперь очевидно, что это невозможно, поскольку повторение такого процесса приведет в конце концов к уравнению, в котором  $k = 1$ , тогда как мы только что показали, что равенство  $k = 1$  невозможно. Это завершает доказательство случая II.

Куммер заявляет, что доказана невозможность равенства  $x^\lambda + y^\lambda = z^\lambda$  для круговых целых (а не только для целых чисел), но здесь в его доказательстве этой теоремы имеется пробел. Приведенное только что доказательство показывает, что если  $x$ ,  $y$  и  $z$  — попарно взаимно простые круговые целые и одно из них делится на  $\alpha - 1$ , то, действительно, равенство  $x^\lambda + y^\lambda = z^\lambda$  невозможно. Кроме того, Куммер был в состоянии так видоизменить свое доказательство случая I, чтобы оно было применимо к тройке  $x$ ,  $y$ ,  $z$  взаимно простых круговых целых (см. упр. 2). Ошибочным является сделанное им предположение, что достаточно доказать теорему в случае, когда  $x$ ,  $y$ ,  $z$  взаимно просты. Иными словами, Куммер действительно доказал, что равенство  $x^\lambda + y^\lambda = z^\lambda$  невозможно для взаимно простых круговых целых, однако упустил из виду, что общий случай не сводится к случаю, когда  $x$ ,  $y$ ,  $z$  взаимно просты. Проблема, разумеется, в том, что  $x$ ,  $y$ ,  $z$  могут иметь общий *идеальный* делитель — дивизор, который делит их все, но не является главным, и на который нельзя сократить равенство  $x^\lambda + y^\lambda = z^\lambda$ . (Доказательство невозможности равенства  $x^\lambda + y^\lambda = z^\lambda$ , в котором этот пробел ликвидирован, см. у Гильберта [НЗ].) То, что сам изобретатель теории идеальных делителей совершил именно этот промах, весьма примечательно.

Остается показать, что если  $e$  — произвольная единица, то  $e/\bar{e} = \alpha^r$  при некотором  $r$ . Выберем полином  $E(X) = a_0 + a_1 X +$

$\dots + a_{\lambda-1}X^{\lambda-1}$  от одной переменной  $X$  с целыми коэффициентами таким образом, чтобы значение  $E(\alpha)$  равнялось единице  $e/\bar{e}$ . Разделим полином  $E(X^{\lambda-1})E(X)$  на  $X^\lambda - 1$  с остатком:  $E(X^{\lambda-1})E(X) = Q(X)(X^\lambda - 1) + R(X)$ , где  $R(X)$  — полином степени меньшей  $\lambda$ , скажем  $R(X) = A_0 + A_1X + \dots + A_{\lambda-1}X^{\lambda-1}$ . Подставляя в это равенство  $X = 1$ , найдем, что  $(a_0 + a_1 + \dots + a_{\lambda-1})^2 = A_0 + A_1 + \dots + A_{\lambda-1}$ . При  $X = \alpha$  получим  $A_0 + A_1\alpha + \dots + A_{\lambda-1}\alpha^{\lambda-1} = E(\alpha^{-1})E(\alpha) = [e(\alpha^{-1})/\bar{e}(\alpha^{-1})] \times [e(\alpha)/\bar{e}(\alpha)] = [\bar{e}/e][e/\bar{e}] = 1$ ,  $(A_0 - 1) + A_1\alpha + A_2\alpha^2 + \dots + A_{\lambda-1}\alpha^{\lambda-1} = 0$ , откуда  $A_0 - 1 = A_1 = A_2 = \dots = A_{\lambda-1}$ . Обозначим через  $k$  это общее значение. Тогда  $(a_0 + a_1 + \dots + a_{\lambda-1})^2 = 1 + \lambda k \equiv 1 \pmod{\lambda}$  и  $a_0 + a_1 + \dots + a_{\lambda-1} \equiv \pm 1 \pmod{\lambda}$ . Прибавляя ко всем коэффициентам (или вычитая) одно и то же целое число, мы можем получить равенство  $a_0 + a_1 + \dots + a_{\lambda-1} = \pm 1$ . Это заменяет первоначальный полином  $E(X)$  и дает новый набор коэффициентов  $A_i$ , для которых  $1 + k\lambda = 1$ ,  $k = 0$ ,  $A_0 = 1$ ,  $A_1 = A_2 = \dots = A_{\lambda-1} = 0$ . С другой стороны, способ подсчета коэффициентов  $A_i$  показывает, что  $A_0 = a_0^2 + a_1^2 + \dots + a_{\lambda-1}^2$ . Эту формулу можно доказать, заметив, что общий член  $a_iX^{\lambda i - i} a_jX^j$  полинома  $E(X^{\lambda-1})E(X)$  может быть записан в виде  $a_i a_j X^{q\lambda + r} = a_i a_j X^r (X^{q\lambda} - 1) + a_i a_j X^r = Q_{i,j}(X)(X^\lambda - 1) + a_i a_j X^r$ , где  $r \equiv j - i \pmod{\lambda}$ ,  $0 \leq r < \lambda$  и  $Q_{i,j}(X) = a_i a_j X^r (X^{q\lambda - \lambda} + \dots + X^\lambda + 1)$  при  $q > 1$ ,  $Q_{i,j}(X) = a_i a_j X^r$  при  $q = 1$  и  $Q_{i,j}(X) = 0$  при  $q = 0$ . Если просуммировать эти равенства по всем  $i$  и  $j$  от 0 до  $\lambda - 1$ , то получим  $R(X) = \sum_{r=0}^{\lambda-1} \left( \sum_{j-i \equiv r} a_i a_j \right) X^r$ . В частности,  $A_0 = a_0^2 + a_1^2 + \dots + a_{\lambda-1}^2$ . Таким образом, из  $A_0 = 1$  вытекает, что точно один коэффициент  $a_i$  отличен от нуля и что он равен  $\pm 1$ . Следовательно,  $E(\alpha) = \pm \alpha^r$  для некоторого  $r$ . Теперь достаточно доказать, что равенство  $E(\alpha) = -\alpha^r$  невозможно. Если бы оно было возможно, то, поскольку либо  $r$ , либо  $r + \lambda$  четно, было бы возможно равенство  $E(\alpha) = -\alpha^{2s}$ , откуда  $e\alpha^{-s} = -\bar{e}\alpha^s$ . Обозначим эту единицу  $e\alpha^{-s}$  через  $F(\alpha) = b_0 + b_1\alpha + \dots + b_{\lambda-1}\alpha^{\lambda-1}$ . Тогда  $F(\alpha)$  — такая единица, что  $F(\alpha) = -F(\alpha^{-1})$ . Предположим, не умаляя общности, что  $b_0 = 0$ . Тогда  $F(\alpha) = b_1(\alpha - \alpha^{-1}) + b_2(\alpha^2 - \alpha^{-2}) + \dots$ . Это показывает, что  $F(\alpha)$  делится на  $\alpha - \alpha^{-1}$ , что невозможно, поскольку  $\alpha - \alpha^{-1}$  не является единицей. Этим доказательство завершается.

## Упражнения

1. Докажите, что каждое круговое целое сравнимо по модулю  $\alpha - 1$  с обычным целым числом. (Вспомните признак делимости на  $\alpha - 1$ .) Установите, что для любого данного кругового целого  $x$  и любого целого числа

$k > 0$  существуют такие целые числа  $a_0, a_1, \dots, a_{k-1}$ , что  $x \equiv a_0 + a_1(\alpha - 1) + \dots + a_{k-1}(\alpha - 1)^{k-1} \pmod{(\alpha - 1)^k}$ . Наконец, покажите, что если  $k \leq \lambda - 1$ , то целые числа  $a_0, a_1, \dots, a_{k-1}$  определены однозначно по модулю  $\lambda$ . (Целое число тогда и только тогда является нулем по модулю  $\alpha - 1$ , когда оно делится на  $\lambda$ . В этом случае оно является нулем и по модулю  $(\alpha - 1)^{\lambda-1}$ .)

2. Докажите, что если  $\lambda$  — регулярное простое число, большее 3, и если  $x, y$  и  $z$  — взаимно простые круговые целые, то равенство  $x^\lambda + y^\lambda = z^\lambda$  невозможно. (Случай, когда одно из неизвестных делится на  $\alpha - 1$ , охватывается доказательством случая II, которое дано в тексте, так что остается лишь случай I. Заменяя, если это необходимо,  $x$  на  $\alpha^v x$ , мы можем вначале предположить, что  $x$  сравним по модулю  $(\alpha - 1)^2$  с целым числом и то же самое верно для  $y$  и  $z$ . Пусть, скажем,  $x \equiv a, y \equiv b, z \equiv c \pmod{(\alpha - 1)^2}$ , где  $a, b, c$  — целые числа. Доказательство, приведенное в тексте, показывает, что для каждого  $j$  имеется такое  $r$ , что  $x + \alpha^{-j}y \equiv \alpha^{-r}(\bar{x} + \alpha^j\bar{y})$ . Далее, используя запись  $\alpha^j = [1 + (\alpha - 1)]^j$  и проводя вычисления по модулю  $(\alpha - 1)^2$ , находим, что  $r(a + b) \equiv 2jb \pmod{\lambda}$ . Отсюда видно, что  $r \equiv vj \pmod{\lambda}$ , где  $v$  — целое число, не зависящее от  $j$ . В действительности можно считать  $v$  четным, так что наше сравнение примет симметричный вид:  $\alpha^{kj}(x + \alpha^{-j}y) \equiv \alpha^{-kj}(\bar{x} + \alpha^j\bar{y}) \pmod{\lambda}$ . В частности,  $x + y \equiv \bar{x} + \bar{y} \pmod{\lambda}$ . Если первоначальному уравнению придать симметричный вид  $x^\lambda + y^\lambda + z^\lambda = 0$ , то, применяя те же соображения к парам  $x, z$  и  $y, z$ , получим  $x \equiv \bar{x}, y \equiv \bar{y}, z \equiv \bar{z} \pmod{\lambda}$ . Значит, выражение  $\alpha^{kj}(x + \alpha^{-j}y)$  не изменяется по модулю  $\lambda$ , если  $j$  заменить на  $-j$ . Из случаев  $j = 1$  и  $j = 2$  мы можем заключить, что так как  $y$  не содержит множителя  $\alpha - 1$ , то  $(\alpha^{k-1} - \alpha^{-(k-1)})(\alpha^{-k} - \alpha^{k-1})(1 - \alpha)$  делится на  $(\alpha - 1)^{\lambda-1}$ . Но  $\lambda \geq 5$ , поэтому либо  $\alpha^{k-1} = \alpha^{-(k-1)}$ , либо  $\alpha^{-k} = \alpha^{k-1}$ , т. е. либо  $k \equiv 1 \pmod{\lambda}$ , либо  $2k \equiv 1 \pmod{\lambda}$ . В первом случае  $a \equiv 0$  вопреки предположению. Во втором случае  $a \equiv b$ . Таким образом, вдобавок к полученному имеем  $a \equiv c$  и  $0 = x^\lambda + y^\lambda + z^\lambda \equiv a^\lambda + b^\lambda + c^\lambda \equiv 3a$ , и снова  $a \equiv 0$  вопреки предположению.)

## 5.6. Квадратичная взаимность

Очень странно, что Куммер так и не разработал полностью связь между своей теорией и гауссовой теорией бинарных квадратичных форм. Это тем более удивительно, поскольку знаменитая теорема о квадратичной взаимности является простым следствием его теории. Гаусс считал эту теорему настолько важной, что назвал ее «фундаментальной теоремой» и опубликовал несколько ее доказательств — два в «Арифметических исследованиях» и четыре других впоследствии (см. [G5]). Сам Куммер, как уже упоминалось в § 4.1, считал квадратичный закон взаимности и его обобщения на высшие степени важнейшим разделом теории чисел. Почти непостижимо, чтобы он мог проглядеть ту простую дедукцию квадратичной взаимности из теории идеальной факторизации<sup>1)</sup>, которую мы сейчас изложим. Скорее нужно предположить,

<sup>1)</sup> Согласно Гекке ([H2], стр. 113), это доказательство впервые дано Кронекером, учеником и близким другом Куммера [*Berlin Monatsberichte*, 1880, 404—408].



что он предпочитал не публиковать ничего по этому вопросу, пока не разработал обобщений на высшие степени, что ему удалось сделать несколько лет спустя. Теория бинарных квадратичных форм связана с квадратичной взаимностью, но не связана с высшими законами взаимности, поэтому она осталась в стороне и в более поздних публикациях Куммера, посвященных законам взаимности.

Рассмотрим снова пример  $\lambda = 23$ , который мы так подробно изучали в § 5.2. В связи с этим примером весьма естественно возникает вопрос: для каких простых  $p$  дивизор числа  $p$  содержит сомножитель вида  $(p, u)$ ? На самом деле полное решение задачи из § 5.2, вероятно, должно содержать ответ на этот вопрос.

В § 5.2 мы обошли его только потому, что это увело бы нас там в сторону от главной цели — обоснования определения эквивалентности дивизоров. Тщательное изучение этого вопроса почти неизбежно ведет к квадратичному закону взаимности.

В § 5.2 уже было замечено, что дивизор  $(p, u)$  имеется *тогда и только тогда, когда  $p$  имеет четное число простых дивизоров*. (Здесь и во всем дальнейшем обсуждении предполагается, что  $p \neq 23$ .) Действительно, с одной стороны, если разложение дивизора  $p$  имеет вид  $(p, u)(p, -1 - u)$ , то, поскольку сопряжение  $\alpha \mapsto \alpha^{-2}$  меняет местами простые дивизоры  $(p, u)$  с простыми дивизорами  $(p, -1 - u)$ , эти два дивизора должны расщеплять простые дивизоры числа  $p$  на два подмножества одинаковой мощности и число всех простых дивизоров должно быть четным. С другой стороны, если их четное число, то число  $e = 22/f$  делится на 2, откуда следует, что  $f$  делит 11. Следовательно, поскольку периоды длины  $f$  сравнимы по модулю любого простого дивизора числа  $p$  с целыми числами, период  $\theta_0$  сравним с некоторым целым числом. Пусть  $\theta_0$  сравним с  $u$  по модулю некоторого конкретного простого дивизора  $p$ . Тогда точно половина простых дивизоров числа  $p$  делит  $\theta_0 - u$ , а их произведение есть дивизор вида  $(p, u)$ , что и требовалось показать.

Это необходимое и достаточное условие существования дивизора  $(p, u)$  можно переформулировать следующим образом. Во-первых,  $e$  тогда и только тогда четно, когда  $f$  делит 11. Так как  $f$ , по определению, есть показатель числа  $p$  по модулю 23, то это тогда и только тогда верно, когда  $p^{11} \equiv 1 \pmod{23}$ . Далее, согласно хорошо известному утверждению из теории чисел, называемому критерием Эйлера, сравнение  $x^{(\lambda-1)/2} \equiv 1 \pmod{\lambda}$  тогда и только тогда имеет место, когда  $x$  является ненулевым квадратом по модулю  $\lambda$ , т. е. тогда и только тогда, когда имеется такое  $y \not\equiv 0 \pmod{\lambda}$ , что  $x \equiv y^2 \pmod{\lambda}$ . Это легко доказать многими способами (см. упр. 7), а отсюда в нашем случае вытекает, что если  $p \neq 23$ , то дивизор вида  $(p, u)$  имеется для тех и только тех  $p$ , которые являются квадратами по модулю 23.

Квадратами по модулю 23 являются:  $1, 4, 9, 16 \equiv -7, 25 \equiv 2, 36 \equiv -10, 49 \equiv 3, 64 \equiv -5, 81 \equiv -11, 100 \equiv 8, 121 \equiv 6$ , или, в более удобном порядке:  $1, 2, 3, 4, -5, 6, -7, 8, 9, -10, -11$ . Тогда из последовательности простых чисел  $2, 3, 5, 7, 11, \dots$  легко выделить те простые, для которых имеются дивизоры  $(p, u)$ :  $2, 3, 13 \equiv -10, 29 \equiv 6, 31 \equiv 8, 41 \equiv -5, \dots$ . Этот список, конечно, согласуется с табл. 5.2.2.

Однако эти соображения не обеспечивают нас значением  $u$  для каждого значения  $p$ ; на самом же деле именно поиск значений  $u$  приводит к другому критерию существования дивизора  $(p, u)$ . Основное свойство целого числа  $u$  состоит в том, что половина простых дивизоров числа  $p$  делит  $\theta_0 - u$ . Тогда все простые дивизоры числа  $p$ , а поэтому и само  $p$ , делят  $(\theta_0 - u)(\theta_1 - u) = u^2 + u + 6$ . Следовательно,  $u$  — решение сравнения  $u^2 + u + 6 \equiv 0 \pmod{p}$ . Связь этого сравнения с  $\lambda = 23$  становится яснее, если записать его в виде  $1/4 [(2u + 1)^2 + 23] \equiv 0 \pmod{p}$ . Это показывает, что если имеется дивизор вида  $(p, u)$ , то  $(2u + 1)^2 \equiv -23$ , и, в частности, что  $-23$  является квадратом по модулю  $p$ . Верно также и обратное, если исключить простое число  $p = 2$ . Если  $p \neq 2$  и  $x^2 \equiv -23 \pmod{p}$ , то  $(x + p)^2 \equiv -23 \pmod{p}$  и либо  $x$ , либо  $x + p$  нечетно. Тогда имеется такое  $u$ , что  $(2u + 1)^2 \equiv -23 \pmod{p}$ . Отсюда вытекает, что  $p$  делит  $(2u + 1)^2 + 23 = 4(\theta_0 - u)(\theta_1 - u)$ , а так как  $p \neq 2$ , то каждый простой дивизор числа  $p$  делит либо  $\theta_0 - u$ , либо  $\theta_1 - u$  и, следовательно, дивизор вида  $(p, u)$  имеется. Короче, если  $p \neq 23$  и  $p \neq 2$ , то дивизор вида  $(p, u)$  имеется в том и только том случае, когда  $-23$  есть квадрат по модулю  $p$ .

Сопоставление этих двух критериев существования дивизора  $(p, u)$  обнаруживает удивительное обстоятельство, что простое число  $p \neq 2$  и  $p \neq 23$  тогда и только тогда является квадратом по модулю 23, когда  $-23$  является квадратом по модулю  $p$ . Это — один случай квадратичного закона взаимности. Другие случаи легко получить, обобщая предыдущие соображения на  $\lambda$ , отличные от 23.

Если сказано, что в круговых целых для данного  $\lambda$  имеется дивизор вида  $(p, u)$ , это означает, что для этого  $\lambda$  точно половина простых дивизоров числа  $p$  делит  $\theta_0 - u$  (где  $\theta_0$  — тот период длины  $(\lambda - 1)/2$ , который содержит  $\alpha$ ). Точно те же соображения, что и в случае  $\lambda = 23$ , доказывают, что если  $p \neq \lambda$ , то дивизор вида  $(p, u)$  имеется в том и только том случае, когда  $p$  есть квадрат по модулю  $\lambda$ . В общем случае формула, которая при  $\lambda = 23$  имела вид  $(\theta_0 - u)(\theta_1 - u) = 1/4 [(2u + 1)^2 + 23]$ , превращается, как мы далее покажем, в следующую:  $(\theta_0 - u)(\theta_1 - u) = 1/4 [(2u + 1)^2 \pm \lambda]$ , где знак перед  $\lambda$  определяется условием, что 4 должно делить  $(2u + 1)^2 \pm \lambda$ , т. е. стоит знак  $+$ , если  $\lambda \equiv 3 \pmod{4}$ , и знак  $-$ , если  $\lambda \equiv 1 \pmod{4}$ . Далее, те же самые

рассуждения показывают, что при  $p \neq 2$  и  $p \neq \lambda$  дивизор вида  $(p, u)$  имеется тогда и только тогда, когда  $-\lambda$  является квадратом по модулю  $p$ , если  $\lambda \equiv 3 \pmod{4}$ , и когда  $\lambda$  является квадратом по модулю  $p$ , если  $\lambda \equiv 1 \pmod{4}$ . Итак:

*Пусть  $p$  и  $\lambda$  — различные нечетные простые числа ( $p \neq 2$ ,  $\lambda \neq 2$ ,  $p \neq \lambda$ ). Если  $\lambda \equiv 1 \pmod{4}$ , то  $p$  тогда и только тогда является квадратом по модулю  $\lambda$ , когда  $\lambda$  является квадратом по модулю  $p$ . Если  $\lambda \equiv 3 \pmod{4}$ , то  $p$  тогда и только тогда является квадратом по модулю  $\lambda$ , когда  $-\lambda$  есть квадрат по модулю  $p$ .*

Именно в таком виде Гаусс сформулировал *квадратичный закон взаимности*, или, как он его называл, *фундаментальную теорему* [Disquisitiones Arithmeticae, Art. 131]. Заметим, что приведенные выше рассуждения в действительности не только доказывают теорему, но дают простой, хотя и совершенно не отвечающий историческому ходу дела, путь открытия самой *формулировки* теоремы. Осталось только доказать формулу  $(\theta_0 - u) \times (\theta_1 - u) = \frac{1}{4} [(2u + 1)^2 \pm \lambda]$ . Это можно сделать следующим образом. (См. упр. 3 и 4 к § 4.5.)

Конечно,  $(\theta_0 - u)(\theta_1 - u) = u^2 + u + \theta_0\theta_1 = \frac{1}{4} [(2u + 1)^2 + 4\theta_0\theta_1 - 1]$ . Задача, следовательно, заключается в подсчете выражения  $4\theta_0\theta_1 - 1$ . Как было замечено в § 4.9 (для периодов длины  $f$ , где  $f = (\lambda - 1)/2$ ),  $\theta_0\theta_1$  имеет вид  $a \cdot \frac{1}{2} (\lambda - 1) + b\theta_0 + c\theta_1$ , где  $a + b + c = \frac{1}{2} (\lambda - 1)$  и  $a$  есть 0 или 1. По симметрии,  $b = c$ . Если  $a = 0$ , то равенство  $a + b + c = (\lambda - 1)/2$  превращается в  $2b = (\lambda - 1)/2$ ; далее,  $\lambda = 4b + 1$ ,  $\lambda \equiv 1 \pmod{4}$ ,  $\theta_0\theta_1 = a + b\theta_0 + c\theta_1 = 0 + b(\theta_0 + \theta_1) = -b$ ,  $4\theta_0\theta_1 - 1 = -4b - 1 = -\lambda$ . Если  $a = 1$ , то равенство  $a + b + c = (\lambda - 1)/2$  превращается в  $1 + 2b = (\lambda - 1)/2$ ; далее,  $4b + 3 = \lambda$ ,  $\lambda \equiv 3 \pmod{4}$ ,  $\theta_0\theta_1 = \frac{1}{2} (\lambda - 1) + b\theta_0 + b\theta_1 = 1 + 2b - b = b + 1$ ,  $4\theta_0\theta_1 - 1 = 4b + 4 - 1 = \lambda$ . Таким образом, либо  $\lambda \equiv 1 \pmod{4}$  и  $4\theta_0\theta_1 - 1 = -\lambda$ , либо  $\lambda \equiv 3 \pmod{4}$  и  $4\theta_0\theta_1 - 1 = \lambda$ , что и требовалось доказать.

Причина, по которой квадратичный закон взаимности вызвал такое восхищение многих крупных математиков, должна быть очевидна. С первого взгляда не видно абсолютно никакой связи между вопросами «квадрат ли  $p$  по модулю  $\lambda$ ?» и «квадрат ли  $\lambda$  по модулю  $p$ ?», но вот открыта теорема, которая показывает, что это практически один и тот же вопрос. Безусловно, наиболее впечатляющими теоремами в математике являются те, в которых предпосылки обнаруживают наименее заметную связь с заключениями, и квадратичный закон взаимности — образцовый пример такой теоремы. Не только Гаусс и Куммер, но также Эйлер, Лагранж, Лежандр, Дирихле, Якоби, Эйзенштейн, Лиувилль, Гильберт, Артин и многие, многие другие известные математики

приняли брошенный этой теоремой вызов найти ее естественное доказательство или обнаружить какое-то более понятное явление «взаимности», частным случаем которого является эта теорема. Гаусс назвал квадратичный закон взаимности *фундаментальной теоремой*, но не из-за его эстетической ценности, а из-за его очень большой значимости в теории сравнений второй степени и в теории бинарных квадратичных форм, которым посвящены четвертый и пятый разделы его «Арифметических исследований». Как будет видно в гл. 7, этот закон очень полезен и в теории идеальной факторизации квадратичных целых. Особенно часто во всех этих теориях необходимость в нем возникает тогда, когда требуется выяснить, имеет ли сравнение  $n \equiv x^2 \pmod{p}$  решение для данного простого  $p$  и целого  $n \not\equiv 0 \pmod{p}$ . Разумеется, это конечная задача, которую можно решить попросту вычислением квадратов всех целых чисел, меньших  $p/2$ , и проверкой, нет ли среди этих квадратов числа, сравнимого с  $n$  по модулю  $p$ . Однако даже когда применяются некоторые элементарные упрощения (см упр. 1 и 2), при больших простых числах  $p$  это требует длительного процесса проб и ошибок, а использование квадратичного закона взаимности неизмеримо упрощает дело. Опишем способ его применения.

Предположим, например, что требуется определить, обладает ли решением сравнение  $x^2 \equiv 31 \pmod{79}$ . Введем так называемый *символ Лежандра*  $\left(\frac{n}{p}\right)$ , где  $p$  — нечетное (положительное) простое число, а  $n$  — целое число,  $n \not\equiv 0 \pmod{p}$ . По определению, он принимает значения  $\pm 1$ , а именно, он равен  $+1$ , если сравнение  $x^2 \equiv n \pmod{p}$  имеет решение, и равен  $-1$  в противном случае. Задача состоит в вычислении символа Лежандра  $\left(\frac{31}{79}\right)$ . Поскольку  $79 \equiv 3 \pmod{4}$ , квадратичный закон взаимности утверждает, что  $\left(\frac{-79}{31}\right) = \left(\frac{31}{79}\right)$ . Но  $-79 \equiv n \equiv 14 \pmod{31}$ , поэтому  $\left(\frac{31}{79}\right) = \left(\frac{14}{31}\right)$ , и мы сталкиваемся со значительно меньшей задачей — определить, обладает ли решением сравнение  $x^2 \equiv 14 \pmod{31}$ . Как отмечалось в приведенном выше доказательстве, критерий Эйлера утверждает, что  $\left(\frac{n}{p}\right) = +1$  в том и только том случае, когда  $n^{(p-1)/2} \equiv 1 \pmod{p}$ . С другой стороны, квадрат числа  $n^{(p-1)/2}$  равен 1 по модулю  $p$  и, следовательно,  $n^{(p-1)/2}$  может иметь только значения  $+1$  или  $-1$ . Значит,  $\left(\frac{n}{p}\right) = -1$  тогда и только тогда, когда  $n^{(p-1)/2} \equiv -1 \pmod{p}$ . Из этих рассуждений вытекает, что  $n^{(p-1)/2} \equiv \left(\frac{n}{p}\right) \pmod{p}$ , откуда следует, что для символа Лежандра выполняется основное соотношение

$$\left(\frac{n}{p}\right) \left(\frac{m}{p}\right) = \left(\frac{nm}{p}\right)$$

при всех таких  $n$ ,  $m$  и  $p$ , при которых определены  $\left(\frac{n}{p}\right)$  и  $\left(\frac{m}{p}\right)$ . Следовательно, для того чтобы подсчитать  $\left(\frac{14}{31}\right)$ , достаточно под-

считать  $\binom{2}{31}$  и  $\binom{7}{31}$ . На основании квадратичной взаимности  $\binom{-31}{7} = \binom{4}{7} = \binom{2}{7} \binom{2}{7} = (\pm 1)^2 = 1$ , а это дает  $\binom{31}{79} = \binom{2}{31}$ . Это допускает дальнейшее приведение:  $\binom{2}{31} = \binom{33}{31} = \binom{3}{31} \binom{11}{31} = \binom{-31}{3} \binom{-31}{11} = \binom{2}{3} \binom{2}{11} = -\binom{2}{11}$ . В результате получается уже совсем несложная задача: квадратами по модулю 11 являются 1, 4,  $9 \equiv -2$ ,  $16 \equiv 5$ ,  $25 \equiv 3$ ,  $49 \equiv 5$ ,  $64 \equiv -2$ ,  $81 \equiv 4$ ,  $100 \equiv 1$ ,  $121 \equiv 0$ . Этот перечень не содержит числа 2, следовательно,  $\binom{2}{11} = -1$ , и окончательно  $\binom{31}{79} = +1$ , т. е. 31 является квадратом по модулю 79.

Применяя этот процесс, полезно располагать так называемыми *дополнительными* законами квадратичной взаимности (в которых элемент взаимности, собственно говоря, отсутствует) для подсчета символов Лежандра  $\binom{-1}{p}$ ,  $\binom{2}{p}$ . Первый закон утверждает:

$$\binom{-1}{p} = \begin{cases} +1, & \text{если } p \equiv 1 \pmod{4}, \\ -1, & \text{если } p \equiv 3 \pmod{4}. \end{cases} \quad (1)$$

Иными словами,  $\binom{-1}{p} = \binom{-1}{p+4n}$ , когда оба выражения определены (т. е. когда  $p+4n$  — положительное простое число), и это остается верным, если положить значение  $\binom{-1}{1}$  равным  $+1$ . Можно проверить, что  $\binom{-1}{3} = -1$ . Второй закон состоит в том, что

$$\binom{2}{p} = \begin{cases} +1, & \text{если } p \equiv 1 \text{ или } 7 \pmod{8}, \\ -1, & \text{если } p \equiv 3 \text{ или } 5 \pmod{8}. \end{cases} \quad (2)$$

Другими словами,  $\binom{2}{p} = \binom{2}{p+8n}$ , и это остается верным, если положить  $\binom{2}{1}$  равным  $+1$ . Можно проверить, что  $\binom{2}{3} = -1$ ,  $\binom{2}{5} = -1$  и  $\binom{2}{7} = +1$ .

Эти два утверждения следуют из теорем, касающихся представлений  $p = a^2 + b^2$  и  $p = a^2 + 2b^2$  и доказанных в гл. 2 (см. ниже упр. 5 и 6). По-другому (1) можно вывести путем применения квадратичной взаимности к  $p$  и 3 следующим образом. Если  $p \equiv 1 \pmod{4}$ , то  $\binom{-3}{p} = \binom{p}{3} = \binom{3}{p} = \binom{-1}{p} \binom{-3}{p}$ , откуда  $\binom{-1}{p} = +1$ , тогда как если  $p \equiv 3 \pmod{4}$ , то  $\binom{-3}{p} = \binom{p}{3} = \binom{-1}{3} \binom{-p}{3} = \binom{-1}{3} \binom{3}{p} = \binom{-1}{3} \binom{-1}{p} \binom{-3}{p}$ , откуда  $\binom{-1}{3} \binom{-1}{p} = +1$  и  $\binom{-1}{p} = \binom{-1}{3} = -1$ . Формулу (2) можно вывести прямым расширением предыдущего доказательства закона взаимности на исключенный случай  $p = 2$ . То, что 2 тогда и только тогда является квадратом по модулю  $\lambda$ , когда его дивизор раскладывается так, как это требуется, верно и в этом случае; с другой стороны, его дивизор



раскладывается тогда и только тогда, когда возможно сравнение  $u^2 + u + \theta_0\theta_1 \equiv 0 \pmod{2}$ . Это равносильно тому, что  $(2u + 1)^2 \pm \lambda \equiv 0 \pmod{8}$ , что зависит лишь от класса числа  $\lambda$  по модулю 8. Если  $\lambda \equiv 1 \pmod{8}$ , то нужное сравнение  $(2u - 1)^2 - 1 \equiv 0 \pmod{8}$  не только возможно, но и справедливо при всех целых  $u$ .

Правилом (1) и символом Лежандра можно воспользоваться для того, чтобы придать квадратичному закону взаимности ясный и симметричный вид: если  $p$  и  $q$  — различные нечетные простые числа и хотя бы одно из них сравнимо с 1 по модулю 4, то  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ ; если же они оба сравнимы с 3 по модулю 4, то  $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$  (поскольку  $\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-p}{q}\right) = -\left(\frac{q}{p}\right)$ ). Таким образом, подсчет символа  $\left(\frac{31}{79}\right)$  можно проще проделать так:  $\left(\frac{31}{79}\right) = -\left(\frac{79}{31}\right) = -\left(\frac{17}{31}\right) = -\left(\frac{31}{17}\right) = -\left(\frac{14}{17}\right) = -\left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = -\left(\frac{2}{1}\right)\left(\frac{17}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = +1$ .

## Упражнения

1. Решите сравнение  $x^2 \equiv 31 \pmod{79}$ . (Сделайте это методом проб и ошибок. Вместо того чтобы вычислять квадраты, можно последовательно прибавлять нечетные числа:  $2^2 = 1^2 + 3$ ,  $3^2 = 2^2 + 5$ ,  $4^2 = 3^2 + 7$ , ..., затем редуцировать по модулю 79.)

2. Гаусс предлагает следующий метод решения сравнений  $x^2 \equiv A \pmod{m}$  (Disquisitiones Arithmeticae, Art. 319—322). Напишем  $x^2 = A + my$  и будем рассматривать  $y$  как неизвестное. Можно считать, что  $-A/m \leq y < 1/4 m - (A/m)$ . Для любых модулей  $E$  (которые Гаусс называет *исключающими*) число  $A + my$  должно быть сравнимо с квадратом по модулю  $E$ . Только около половины возможных классов по модулю  $E$  являются квадратами, и этим способом можно исключить около половины возможных значений неизвестного  $y$ . Покажите, что в упр. 1 этим способом при  $E = 3, 4$  и  $5$  исключаются все положительные значения  $y$ , кроме четырех, и найдите их. Покажите, что использование  $E = 8$  вместо  $E = 4$  исключает одно из них, а использование  $E = 7$  исключает второе. Испробуйте оставшиеся два.

3. Покажите, что  $\left(\frac{22}{97}\right) = +1$ , и решите сравнение  $x^2 \equiv 22 \pmod{97}$ . ( $E = 8, 9, 5$  исключают все значения, кроме трех, из которых два меньших легко отбрасываются.)

4. Подсчитайте следующие символы Лежандра:  $\left(\frac{79}{101}\right)$ ,  $\left(\frac{97}{139}\right)$ ,  $\left(\frac{91}{139}\right)$ . (Предостережение: о подсчете  $\left(\frac{91}{139}\right) = -\left(\frac{139}{91}\right) = -\left(\frac{48}{91}\right) = -\left(\frac{3}{91}\right) = \left(\frac{91}{3}\right) = +1$  не было доказано, что он верен, хотя он и дает правильный ответ.)

5. Выведите правило (1) для подсчета  $\left(\frac{-1}{p}\right)$  из формул (4) и (5) § 2.4.

6. Докажите правило (2) для подсчета  $\left(\frac{2}{p}\right)$  следующим образом. Упр. 4 к § 2.4 показывает, что если  $\left(\frac{2}{p}\right) = +1$ , то  $p = c^2 - 2d^2$  и, следовательно,  $p \equiv \pm 1 \pmod{8}$ . Обратное доказано в упр. 6 и 7 к § 2.4.



7. Докажите, что формула  $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}$  имеет место, если символ Лежандра определен. (Это легко сделать, используя существование примитивного корня по модулю  $p$ , но избежать использования примитивного корня можно *путем подсчета*: так как возведение в квадрат есть «два в один»-функция, то точно половина ненулевых классов по модулю  $p$  являются квадратами. На основании других соображений произведение квадрата на неквадрат есть неквадрат и, следовательно, произведение двух неквадратов есть квадрат, и т. д.) Установите, что  $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$ .

8. Предположив, что верна вторая формулировка квадратичного закона взаимности (если  $p$  и  $q$  — нечетные простые числа и  $p \equiv 1$  или  $q \equiv 1 \pmod{4}$ , то  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ , но если  $p \equiv 3 \pmod{4}$  и  $q \equiv 3 \pmod{4}$ , то  $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ ), выведите первую (если  $p \equiv 3 \pmod{4}$ , то  $\left(\frac{-p}{q}\right) = \left(\frac{q}{p}\right)$ , а если  $p \equiv 1 \pmod{4}$ , то  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ ). Не пользуйтесь правилом (1), не доказав его сначала.

9. Покажите, что квадратичный закон взаимности можно сформулировать так:  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ .

10. Определите, обладают ли решениями сравнения

$$3u^2 - 2u \equiv 7 \pmod{23},$$

$$7u^2 + 6u \equiv 2 \pmod{37}.$$

[Дополните до квадрата и примените квадратичную взаимность.]

11. Как заметил Лагранж [L1, Art. 54], если  $p \equiv 3 \pmod{4}$ ,  $p$  — простое число и сравнение  $x^2 \equiv B \pmod{p}$  обладает решением, то класс  $x \equiv \equiv B^{(p+1)/4} \pmod{p}$  удовлетворяет сравнению  $x^2 \equiv B$ . Докажите этот факт и воспользуйтесь им для решения упр. 1. Гауссов метод исключения не очень практичен. Относительно лучшего метода см. Шенкс [S1].

## Глава 6

# ОПРЕДЕЛЕНИЕ ЧИСЛА КЛАССОВ

### 6.1. Введение

В апреле 1847 г. Куммер опубликовал свое доказательство того, что из условий <sup>1)</sup> (A) и (B) для заданного показателя  $\lambda$  вытекает Последняя теорема Ферма. Для того чтобы применить эту теорему к доказательству самой теоремы Ферма для конкретного простого показателя  $\lambda$ , нужно иметь какой-нибудь способ проверки условий (A) и (B) для данного  $\lambda$ . Куммер утверждал, что им строго доказано выполнение этих условий для  $\lambda = 3, 5, 7$  и что они, по-видимому, выполняются хотя и не для всех простых  $\lambda$ , но для бесконечного множества их. Естественный путь подойти к проверке условия (A) — попытаться сосчитать число классов для данного значения  $\lambda$ . Эту задачу определения числа классов Куммер упомянул уже в своем самом первом сообщении 1847 г. по теории идеальных комплексных чисел, однако лишь затем, чтобы сказать, что он ею не занимался, поскольку ему устно сообщили, что Дирихле уже преуспел в нахождении формулы для числа классов. Куммер еще раз сослался на этот факт, когда сообщал Дирихле о своей апрельской работе 1847 г., говоря, что сам он не в состоянии сказать, какие простые  $\lambda$  удовлетворяют условиям (A) и (B), «но для Вас это, вероятно, не составит труда». Однако Дирихле в замечаниях, которые он сделал к этому сообщению, говорит лишь, что у него есть формула для числа классов, позволяющая в частных случаях проверять, выполнено ли условие (A); он не приводит никаких значений  $\lambda$ , для которых он проверил это условие, и признает, что этот способ проверки непрактичен для условия (B) при  $\lambda > 7$  и что он не в состоянии сказать, верна ли гипотеза Куммера о том, что (B) вытекает из (A). Наконец, в сентябре 1847 г. Куммер послал Дирихле и в Берлинскую Академию статью [K10], в которой дал вполне исчерпывающую теорему относительно условий (A) и (B).

**Теорема.** Из (A) вытекает (B). Условие (A) равносильно утверждению, что  $\lambda$  не делит числители ни одного из чисел Бернулли

---

<sup>1)</sup> Эти условия таковы: (A) число классов не делится на  $\lambda$ ; (B) любая единица, сравнимая по модулю  $\lambda$  с целым числом, является  $\lambda$ -й степенью.

$B_2, B_4, \dots, B_{\lambda-3}$  (числа Бернулли определяются <sup>1)</sup>) равенством

$$\frac{x}{e^x - 1} = \sum \frac{B_n x^n}{n!}.$$

Эта теорема и известные значения чисел Бернулли дали Куммеру возможность сказать, что (А) и (В) выполняются для всех простых чисел, меньших 37, но что они не имеют места для  $\lambda = 37$ , поскольку 37 делит числитель  $B_{32}$ . Находить значения чисел Бернулли совсем не просто, но во времена Куммера они были протабулированы вплоть до  $B_{60}$ , и это позволило проверить все простые числа  $\lambda$  до  $\lambda = 61$ . Но Куммер, по-видимому, не провел такой проверки, прежде чем послал свою статью в Берлин, поскольку он не сообщает о том факте, что единственным вторым простым  $\lambda \leq 61$ , для которого (А) и (В) не выполняются, является  $\lambda = 59$ .

При всем почтении Куммера к Дирихле и его признании, что он получил лично от Дирихле некоторую полезную информацию, успешное нахождение им в течение лета 1847 г. как формулы для числа классов, так и приведенной выше теоремы относительно условий (А) и (В), следует рассматривать как невероятное достижение. Читатель сам сможет судить об уровне вычислительного мастерства и упорства, необходимых, чтобы получить результаты этой главы — а они все являются результатами Куммера — между маем и сентябрем одного и того же года.

## 6.2. Формула эйлерова произведения

В основе фактически всей аналитической теории чисел, в которой формула числа классов играет важную роль, лежит *формула эйлерова произведения*

$$\sum_n \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}} \quad (s > 1). \quad (1)$$

Здесь суммирование слева ведется по всем положительным целым  $n = 1, 2, 3, \dots$ , а произведение справа распространяется на все простые  $p = 2, 3, 5, 7, 11, \dots$ . Легко показать, что как произведение, так и сумма сходятся для положительных вещественных чисел  $s$ , больших 1. Доказательство того, что они равны, является простым упражнением по использованию абсолютной сходимости и основной теоремы арифметики (каждое положительное целое число  $n$  точно одним способом может быть записано в виде произведения степеней простых чисел:  $n = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}$ ) для про-

<sup>1)</sup> Куммер пользуется другим определением чисел Бернулли, и его  $B_j$  здесь обозначены через  $B_{2j}$ .

верки справедливости формальных преобразований:

$$\begin{aligned} \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} &= \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \\ &= \sum_{\substack{p \\ \mu_1, \mu_2, \dots}} \frac{1}{p_1^{\mu_1 s} p_2^{\mu_2 s} \dots p_k^{\mu_k s}} = \sum_n \frac{1}{n^s}. \end{aligned}$$

Из этой формулы непосредственно следует бесконечность множества простых чисел, поскольку из  $\sum n^{-s} > \int_1^\infty x^{-s} dx = (s-1)^{-1}$

вытекает, что левая часть равенства (1) стремится к  $\infty$  при  $s \downarrow 1$ , а этого не могло бы быть, если бы произведение в правой части содержало лишь конечное число сомножителей.

Говоря коротко, идея вывода формулы числа классов заключается в следующем. Будем искать аналог формулы (1), когда вместо основной теоремы арифметики для положительных целых чисел рассматривается тривиальное утверждение о том, что дивизор может быть записан точно одним способом в виде произведения простых дивизоров. Так как норма произведения есть произведение норм, то это нам даст

$$\sum_A \frac{1}{N(A)^s} = \prod_P \frac{1}{1 - \frac{1}{N(P)^s}}, \quad (2)$$

где  $A$  пробегает все дивизоры, а  $P$  — все простые дивизоры. Функция от  $s$  в этом равенстве стремится к  $\infty$  при  $s \downarrow 1$  как постоянная, умноженная на  $(s-1)^{-1}$ . Постоянную можно подсчитать двумя способами — по-разному для каждой части равенства; то, что получится слева, включит в себя число классов, а справа — не включит. Приравнивание этой постоянной, подсчитанной двумя способами, и даст *формулу числа классов*. Написать формулу числа классов в замкнутой форме не так легко и требует длинных выкладок (см. § 6.14), однако все это делается на основе только одной этой несложной идеи.

На формулу эйлера произведения опираются многие работы Дирихле, включая его знаменитую теорему о бесконечности количества простых чисел в арифметической прогрессии и его столь же важную формулу для числа классов бинарных квадратичных форм с заданным детерминантом. Действительно, в обеих теоремах проводится исследование, как стремятся к  $\infty$  при  $s \downarrow 1$  функции, аналогичные функции  $\sum n^{-s}$ . Таким образом, идея Куммера богата прецедентами, и исторический подход, подобный принятому в этой книге, казалось бы, требует исследования этих прецедентов с тем, чтобы раскрыть основные замыслы в их простейшей форме.

Однако подробное изучение работы Дирихле скорее мешает, чем помогает усилиям показать идеи в их простейшей форме. Причина этого в том, что Дирихле, следуя Гауссу, формулировал определение числа классов в терминах бинарных квадратичных форм. Лишь в работах Куммера выяснилось, что эту теорию можно изложить значительно изящнее на языке дивизоров (идеальных комплексных чисел), благодаря чему стало возможным увидеть *прямую* связь (менее прямая связь была понятна и Дирихле) между формулой эйлера произведения и формулой Дирихле числа классов. В терминах теории Куммера формула Дирихле есть не что иное, как предельный случай при  $s \downarrow 1$  обобщения (2) формулы (1), когда дивизоры и простые дивизоры, встречающиеся в (2), берутся из арифметики квадратичных целых  $x + y \sqrt{D}$  (см. гл. 9).

По этой причине естественно пропустить работу Дирихле и перейти прямо от формулы эйлера произведения к куммерову обобщению (2) в случае круговых целых. Достаточно отметить, что работа Дирихле дала много ценных указаний, в каких направлениях следует двигаться дальше. Из нее выяснилась не только важность предельного перехода  $s \downarrow 1$ , но и тот факт, что если сумма  $\sum N(A)^{-s}$  разбита в конечное число частичных сумм по *классам эквивалентности* дивизоров  $A$ , то предел при  $s \downarrow 1$  каждой из этих частичных сумм будет одним и тем же, и т. д. Добавим, что Куммер признавал полезность советов, полученных им от Дирихле при обсуждениях, касающихся нахождения числа классов.

Однако в письме Якоби от 27 сентября 1847 г. Куммер говорит: «По-видимому, я вывел эту формулу совершенно не так, как Дирихле, поскольку я никогда не сталкивался с теми трудностями, о которых говорил Дирихле. Трудности, которые преодолевал я, носили более субъективный характер и заключались лишь в малоинтересных выкладках такого типа, с которым я столкнулся, применяя технику, уже изложенную Дирихле в его исследовании квадратичных форм». Далее он говорит, что не решается публиковать свой вывод формулы, поскольку, сделав это, он мог бы лишиться математический мир работы Дирихле, которому он, Куммер, не может никоим образом дать ничего равноценного.

Наконец, Дирихле так и не опубликовал никакого обобщения своей формулы числа классов, выходящего за рамки квадратичного случая. Было бы, конечно, интересно узнать, какую форму приняло бы такое обобщение, но скорее из чистого любопытства, чем по каким-либо математическим соображениям. Кажется более правдоподобным, что без упрощающих дело понятий теории Куммера результаты Дирихле были более трудными и менее общими, чем результаты Куммера, и именно поэтому Дирихле не публиковал их.

### 6.3. Первые шаги

Как было обрисовано в предыдущем параграфе, формула числа классов выводится исследованием предельного перехода при  $s \downarrow 1$  в формуле эйлерова произведения

$$\sum_A N(A)^{-s} = \prod_P (1 - N(P)^{-s})^{-1} \quad (s > 1), \quad (1)$$

где  $A$  пробегает все дивизоры круговых целых, а  $P$  пробегает все *простые* дивизоры (круговые целые соответствуют некоторому фиксированному простому  $\lambda > 2$ , для которого ищется число классов). Этот параграф посвящен простому доказательству формулы эйлерова произведения (1) и основному факту, относящемуся к дзета-функции Римана.

Первым шагом является доказательство того, что произведение в правой части (1) сходится для всех  $s > 1$ . Имеем  $N(P)^{-s} > 0$  (это число равно  $p^{-fs}$ , где  $p$  — простое число, делящееся на  $P$ , а  $f$  — его показатель по модулю  $\lambda$ ). Поэтому первый шаг следует из основной теоремы о сходимости бесконечных произведений, утверждающей, что это произведение тогда и только тогда сходится, когда сходится ряд  $\sum N(P)^{-s}$ . Для каждого простого числа  $p$  этот ряд содержит  $e \leq \lambda - 1$  членов, равных  $p^{-fs} \leq p^{-s}$ , где  $f$  — показатель числа  $p$  по модулю  $\lambda$  (или  $f = 1$ , если  $p = \lambda$ ) и  $e = (\lambda - 1)/f$  (или  $e = 1$ , если  $p = \lambda$ ). Следовательно, ряд

$$\sum N(P)^{-s} \leq (\lambda - 1) \sum_p \frac{1}{p^s} < (\lambda - 1) \sum_n \frac{1}{n^s}$$

сходится, и сходимость произведения доказана.

Любое из конечных произведений, пределом которых является наше бесконечное произведение, равно сумме *некоторых* слагаемых ряда  $\sum N(A)^{-s}$ , а именно, сумме тех слагаемых  $N(A)^{-s}$ , для которых все простые дивизоры дивизора  $A$  включены в конечное произведение. Это вытекает из перемножения абсолютно сходящихся рядов

$$(1 - N(P)^{-s})^{-1} = 1 + N(P)^{-s} + N(P^2)^{-s} + N(P^3)^{-s} + \dots$$

с последующей перегруппировкой слагаемых. Отсюда ясно, что любая конечная сумма  $\sum N(A)^{-s}$  меньше некоторого частичного произведения  $\prod (1 - N(P)^{-s})^{-1}$ , например меньше произведения по всем простым дивизорам, встречающимся в данной конечной сумме. Следовательно, бесконечная сумма  $\sum N(A)^{-s}$  сходится, и она не превосходит бесконечное произведение. С другой стороны, вся сумма  $\sum N(A)^{-s}$  больше, чем любая сумма, полученная из нее отбрасыванием некоторых слагаемых, и, следовательно,



больше любого частичного произведения. Значит, сумма  $\sum N(A)^{-s}$  больше бесконечного произведения или равна ему. Это доказывает формулу (1).

В ходе вывода формулы числа классов будет необходимо воспользоваться одним простейшим фактом, касающимся формулы эйлерова произведения

$$\sum \frac{1}{n^s} = \prod \frac{1}{1 - \frac{1}{p^s}} \quad (s > 1) \quad (1)$$

для обычных целых чисел, а именно тем, что функция от  $s$ , определенная этим выражением, при  $s \downarrow 1$  стремится к  $\infty$  как  $(s - 1)^{-1}$ . Это можно доказать следующим образом. Функция от  $s$ , определенная равенством (2) при  $s > 1$ , называется <sup>1)</sup> *дзета-функцией Римана* и обозначается через  $\zeta(s)$ . Выражение для  $\zeta(s)$  в левой части равенства (2) дает

$$\int_1^\infty \frac{1}{x^s} dx < \sum_{n=1}^\infty \frac{1}{n^s} < 1 + \int_1^\infty \frac{1}{x^s} dx,$$

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1},$$

откуда непосредственно следует, что  $\lim_{s \downarrow 1} (s - 1) \zeta(s) = 1$ , т. е.  $\zeta(s)$  стремится к  $\infty$  при  $s \downarrow 1$  как  $(s - 1)^{-1}$ , что и требовалось показать.

## Упражнения

1. Функция от  $s$ , определенная формулой (1), называется дзета-функцией круговых целых. Покажите, что она стремится к  $\infty$  при  $s \downarrow 1$  тогда и только тогда, когда сумма обратных величин  $1/p$  всех простых чисел  $p$ , для которых  $p \equiv 1 \pmod{\lambda}$ , расходится. [В сумме  $\sum N(P)^{-s}$  лишь простые с показателем 1 могут давать расходимость.] Как доказал Дирихле, это утверждение верно для всех простых  $\lambda$ .

2. Оцените значение произведения  $(s - 1) \zeta(s)$  при  $s = 1,001$ .

3. Докажите, что сумма обратных величин простых целых чисел, т. е.  $\sum (1/p)$ , есть расходящийся ряд. Эта знаменитая теорема Эйлера была началом аналитической теории чисел.

## 6.4. Преобразование правой части

Формула числа классов получается путем доказательства, что функция от  $s$  в формуле эйлерова произведения при  $s \downarrow 1$  стремится к  $\infty$  как постоянная, умноженная на  $(s - 1)^{-1}$ , и подсчета

<sup>1)</sup> Разумеется, ни Дирихле, ни Куммер так ее не называли, поскольку их деятельность на много лет предшествовала деятельности Римана.

постоянной различными способами в обеих частях равенства. Иными словами, эта формула получается при помощи умножения формулы эйлерова произведения на  $(s - 1)$  и перехода к пределу при  $s \downarrow 1$ . Первый шаг будет состоять в перестройке и преобразовании произведения  $\prod (1 - N(P)^{-s})^{-1}$  в правой части формулы.

Рассматриваемое произведение можно в явном виде переписать как

$$\left(1 - \frac{1}{\lambda^s}\right)^{-1} \prod_{p \neq \lambda} \left(1 - \frac{1}{p^{fs}}\right)^{-e}$$

где в бесконечном произведении  $p$  пробегает все простые числа, отличные от  $\lambda$ , а число  $f$  для каждого  $p$  является, по определению, таким наименьшим положительным целым числом, что  $p^f \equiv 1 \pmod{\lambda}$  и  $e = (\lambda - 1)/f$ . Например, при  $\lambda = 5$  произведение равно члену  $(1 - 5^{-s})^{-1}$ , умноженному на

$$\prod_{p \equiv 1} \left(1 - \frac{1}{p^s}\right)^{-4} \prod_{p \equiv 2} \left(1 - \frac{1}{p^{4s}}\right)^{-1} \prod_{p \equiv 3} \left(1 - \frac{1}{p^{4s}}\right)^{-1} \prod_{p \equiv 4} \left(1 - \frac{1}{p^{2s}}\right)^{-2}$$

где знак  $\equiv$  означает сравнение по модулю 5. Нам будет удобно разложить на множители и перестроить это произведение так, чтобы придать ему следующий вид:

$$\begin{aligned} &= \prod_{p \equiv 1} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1} \times \\ &\quad \times \prod_{p \equiv 2} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{i}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \left(1 + \frac{i}{p^s}\right)^{-1} \times \\ &\quad \times \prod_{p \equiv 3} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{i}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \left(1 + \frac{i}{p^s}\right)^{-1} \times \\ &\quad \times \prod_{p \equiv 4} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} = \\ &= \prod_{p \neq 0} \left(1 - \frac{1}{p^s}\right)^{-1} \times \left[ \prod_{p \equiv 1, 4} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 2, 3} \left(1 + \frac{1}{p^s}\right)^{-1} \right] \times \end{aligned}$$

$$\begin{aligned}
& \times \left[ \prod_{p \equiv 1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 2} \left(1 + \frac{i}{p^s}\right)^{-1} \prod_{p \equiv 3} \left(1 - \frac{i}{p^s}\right)^{-1} \prod_{p \equiv 4} \left(1 + \frac{1}{p^s}\right)^{-1} \right] \times \\
& \times \left[ \prod_{p \equiv 1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 2} \left(1 - \frac{i}{p^s}\right)^{-1} \prod_{p \equiv 3} \left(1 + \frac{i}{p^s}\right)^{-1} \prod_{p \equiv 4} \left(1 + \frac{1}{p^s}\right)^{-1} \right] = \\
& = \prod_{k=0}^3 \left[ \prod_{p \equiv 2} \left(1 - \frac{i^k}{p^s}\right)^{-1} \prod_{p \equiv 2^2} \left(1 - \frac{i^{2k}}{p^s}\right)^{-1} \prod_{p \equiv 2^3} \left(1 - \frac{i^{3k}}{p^s}\right)^{-1} \prod_{p \equiv 2^4} \left(1 - \frac{i^{4k}}{p^s}\right)^{-1} \right]
\end{aligned}$$

где  $i = \sqrt{-1}$ . Точно так же при  $\lambda = 7$  каждый член, отличный от  $(1 - 7^{-s})^{-1}$ , имеет один из четырех видов:  $(1 - p^{-s})^{-6}$ ,  $(1 - p^{-2s})^{-3} = (1 - p^{-s})^{-3} (1 + p^{-s})^{-3}$ ,  $(1 - p^{-3s})^{-2} = (1 - p^{-s})^{-2} \times \times (1 - \omega p^{-s})^{-2} (1 - \omega^2 p^{-s})^{-2}$ , где  $\omega$  — примитивный кубический корень из единицы, либо  $(1 - p^{-6s})^{-1} = (1 - p^{-s})^{-1} (1 - \beta p^{-s})^{-1} \times \times (1 - \beta^2 p^{-s})^{-1} (1 - \beta^3 p^{-s})^{-1} (1 - \beta^4 p^{-s})^{-1} (1 - \beta^5 p^{-s})^{-1}$ , где  $\beta$  — примитивный корень 6-й степени из единицы. [Таким образом,  $\beta^6 = 1$ , но в меньших степенях  $\beta$  не дает 1. Тогда  $\omega$  есть  $\beta^2$  или  $\beta^4$  и  $x^6 - y^6 = (x - y)(x - \beta y) \dots (x - \beta^5 y)$  — см. упр. 1.] Каждое такое разложение можно записывать в виде  $(1 - p^{-s})^{-1} (1 - \beta^j p^{-s})^{-1} \times \times (1 - \beta^{2j} p^{-s})^{-1} \dots (1 - \beta^{5j} p^{-s})^{-1}$  при подходящем выборе показателя  $j = 0, 1, 2, 3, 4, 5$ . ( $\beta^3 = -1$ . Разложения при  $j = 1$  и  $j = 5$  совпадают, как и разложения при  $j = 2$  и  $j = 4$ .) Кроме того,  $j$  должно равняться 0, если  $p \equiv 1 \pmod{7}$ , равняться 3, если  $p \equiv 6 \pmod{7}$ , равняться 2 или 4, если  $p \equiv 2$  или  $4 \pmod{7}$ , и 1 или 5, если  $p \equiv 3$  или  $5 \pmod{7}$ . Этого можно достичь, выбирая  $j$  в соответствии с правилом:  $p \equiv 3^j \pmod{7}$ . Тогда

$$\prod (1 - N(P)^{-s})^{-1} = \left(1 - \frac{1}{7^s}\right)^{-1} \prod_{k=0}^5 \prod_{p \equiv 3^k} \left(1 - \frac{\beta^{jk}}{p^s}\right)^{-1}$$

В общем случае формула принимает вид (см. упр. 2)

$$\prod (1 - N(P)^{-s})^{-1} = \left(1 - \frac{1}{\lambda^s}\right)^{-1} \prod_{k=0}^{\lambda-2} \prod_{p \equiv \gamma^k} \left(1 - \frac{\beta^{jk}}{p^s}\right)^{-1} \quad (1)$$

где  $\beta$  — примитивный корень  $(\lambda - 1)$ -й степени из единицы,  $\gamma$  — примитивный корень по модулю  $\lambda$  и во втором произведении умножение производится по всем простым  $p$ , для каждого из которых  $j$  определяется сравнением  $p \equiv \gamma^j \pmod{\lambda}$ .

Произведения  $\prod_{p \equiv \gamma^j} (1 - \beta^{jk} p^{-s})^{-1}$ , входящие в эту формулу, были уже выделены и изучены Дирихле в связи с его работой о простых числах в арифметических прогрессиях. Под *характером по модулю  $\lambda$*  понимается комплекснозначная функция  $\chi$  целого аргумента  $n$ , обладающая свойствами:  $\chi(n + \lambda) = \chi(n)$ ,  $\chi(nt) = \chi(n) \chi(t)$ ,  $\chi(0) = 0$ ,  $\chi(1) \neq 0$ . Простым упражнением является доказательство того, что *имеется точно  $\lambda - 1$  характеров по модулю  $\lambda$*  и что их можно определить следующим образом. Пусть  $\gamma$  — примитивный корень по модулю  $\lambda$  (в приведенных примерах он равен 2, если  $\lambda = 5$ , и 3, если  $\lambda = 7$ ), и пусть  $\beta$  — примитивный корень  $(\lambda - 1)$ -й степени из единицы (в примерах:  $i$ , если  $\lambda = 5$ , и  $\beta$ , если  $\lambda = 7$ ). Тогда для каждого целого  $k$  определим характер  $\chi_k$ , полагая  $\chi_k(\gamma) = \beta^k$ , после чего остальные значения определяются равенствами  $\chi_k(n) = \chi_k(\gamma^j) = \chi_k(\gamma)^j = \beta^{jk}$ , где  $n \equiv \gamma^j \pmod{\lambda}$ ;  $\chi_k(n) = \chi_k(0) = 0$ , если  $n \equiv 0 \pmod{\lambda}$ . Если  $\chi$  — любой характер по модулю  $\lambda$ , то  $\chi(\gamma)^{\lambda-1} = \chi(\gamma^{\lambda-1}) = \chi(1)$ , ибо  $\gamma^{\lambda-1} \equiv 1 \pmod{\lambda}$ . Так как  $\chi(1) \neq 0$  и  $\chi(1)^2 = \chi(1^2) = \chi(1)$ , то  $\chi(1) = 1$ . Значит,  $\chi(\gamma)^{\lambda-1} = 1$  и  $\chi(\gamma)$  должно быть степенью числа  $\beta$ . Так как  $\beta$  имеет точно  $\lambda - 1$  различных степеней и так как  $\chi(\gamma)$  определяет все остальные значения характера  $\chi$ , то отсюда следует, что имеется точно  $\lambda - 1$  характеров по модулю  $\lambda$ , что и требовалось установить.

При этих обозначениях формулу (1) можно переписать так:

$$\prod (1 - N(P)^{-s})^{-1} = \left(1 - \frac{1}{\lambda^s}\right)^{-1} \prod_{\chi} \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

где  $\chi$  пробегает все  $\lambda - 1$  характеров по модулю  $\lambda$ , а  $p$  пробегает все простые числа. (Заметим, что  $\chi(\lambda) = 0$  при всех  $\chi$ .) Дирихле уделил особое внимание этим произведениям по  $p$ , которые он обозначил следующим образом:

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \quad (s > 1)$$

Он заметил, что метод, использованный при выводе формулы эйлерова произведения, дает

$$L(s, \chi) = \sum_n \frac{\chi(n)}{n^s} \quad (s > 1)$$

поскольку, как и раньше,  $(1 - \chi(p) p^{-s})^{-1} = \sum_{\mu=0}^{\infty} [\chi(p) p^{-s}]^{\mu}$  и перемножением этих выражений по всем простым  $p$  получаем

$$\sum \chi(p_1)^{\mu_1} \chi(p_2)^{\mu_2} \dots \chi(p_v)^{\mu_v} p_1^{-\mu_1 s} p_2^{-\mu_2 s} \dots p_v^{-\mu_v s} = \sum \chi(n) n^{-s},$$

ибо  $\chi$  — характер, а каждое положительное целое число  $n$  может быть единственным образом записано в виде  $n = p_1^{\mu_1} p_2^{\mu_2} \dots p_v^{\mu_v}$ . Следовательно, в обозначениях Дирихле правая часть формулы Эйлерова произведения может быть записана так:

$$\prod \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \left(1 - \frac{1}{\lambda^s}\right)^{-1} L(s, \chi_0) L(s, \chi_1) \dots L(s, \chi_{\lambda-2}) \quad (s > 1)$$

где  $\chi_0, \chi_1, \dots, \chi_{\lambda-2}$  — характеры по модулю  $\lambda$ , определенные равенством  $\chi_j(\gamma) = \beta^j$ .

Далее, так как  $\chi_0(p) = 1$  для всех простых  $p$ , исключая  $\lambda$ , и  $\chi_0(\lambda) = 0$ , то первые два члена образуют  $(1 - \lambda^{-s})^{-1} L(s, \chi_0) = \zeta(s)$ , где  $\zeta(s) = \prod (1 - p^{-s})^{-1} = \sum n^{-s}$  — дзета-функция Римана. Следовательно, так как  $\lim_{s \downarrow 1} (s-1) \zeta(s) = 1$  при  $s \downarrow 1$ , то

$$\lim_{s \downarrow 1} (s-1) \prod \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \lim_{s \downarrow 1} L(s, \chi_1) L(s, \chi_2) \dots L(s, \chi_{\lambda-2})$$

и задача определения, каким способом произведение  $\prod (1 - N(P)^{-s})^{-1}$  стремится к  $\infty$  при  $s \downarrow 1$ , сводится к вычислению предела произведения  $L$ -функций Дирихле, стоящего в правой части. Эта задача была уже полностью решена Дирихле, и Куммеру оставалось лишь использовать решение Дирихле. Это решение изложено в следующем параграфе.

## Упражнения

1. Докажите, что если  $\beta$  — примитивный корень  $n$ -й степени из единицы, то  $(x - \beta y)(x - \beta^2 y) \dots (x - \beta^n y) = x^n - y^n$ . Какой вид примет эта формула, если корень  $n$ -й степени из единицы  $\beta$  не является примитивным?

2. Докажите формулу (1).

3. Для  $\lambda = 13$  найдите два характера  $\chi$  по модулю  $\lambda$ , обладающие тем свойством, что все их значения вещественны. Напишите первые 15 членов соответствующего  $L$ -ряда в каждом из этих двух случаев. Напишите первые 10 членов ряда для  $(1 - \chi(2) 2^{-s})^{-1} (1 - \chi(3) 3^{-s})^{-1}$  в каждом из случаев.

4. Определение характера по модулю  $\lambda$  никоим образом не зависит от предположения, что  $\lambda$  — простое число. Следовательно, смысл «характера

по модулю 8» ясен. Найдите 4 вещественнозначных характера по модулю 8 и покажите, что других характеров по модулю 8 не существует.

### 6.5. Проведенное Дирихле вычисление значений $L(1, \chi)$

Пусть  $\lambda$  — данное простое число,  $\lambda > 2$ ,  $\chi$  — характер по модулю  $\lambda$  и  $L(s, \chi)$  обозначает функцию

$$\sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad (s > 1).$$

Характер  $\chi$ , определенный условиями  $\chi(n) = 1$  при  $n \not\equiv 0 \pmod{\lambda}$  и  $\chi(n) = 0$  при  $n \equiv 0 \pmod{\lambda}$ , называется *главным* характером по модулю  $\lambda$ . По причинам, изложенным в предыдущем параграфе, часть вывода формулы Куммера для числа классов заключается в нахождении предела  $\lim_{s \downarrow 1} L(s, \chi)$  для всех  $\lambda \geq 2$  характеров  $\chi$ , *отличных* от главного характера.

Первым шагом в вычислении этого предела будет доказательство того, что ряд  $L(s, \chi) = \sum \chi(n) n^{-s}$  *условно сходится* при  $s > 0$  (предполагается, что  $\chi$  не является главным характером) и что  $L(s, \chi)$  есть корректно определенная непрерывная (в действительности аналитическая) функция при  $s > 0$ . Значит, искомый предел может быть записан в виде  $L(1, \chi) = \sum \chi(n) n^{-1}$ , причем ряд *условно сходится*.

Доказывать, что ряд  $\sum \chi(n) n^{-s}$  *условно сходится* при  $s > 0$ , мы будем методом *суммирования по частям*. Обозначим через  $S(n)$  сумму значений функции  $\chi(n)$ , т. е.  $S(0) = 0$ ,  $S(n) = S(n-1) + \chi(n)$ , так что  $S(n) = \chi(1) + \chi(2) + \dots + \chi(n)$ . Тогда при условии, что  $\chi$  — неглавный характер, имеем  $S(\lambda) = 0$ , поскольку  $S(\lambda)$  есть сумма  $\lambda - 1$  ненулевых значений характера  $\chi$  в некотором порядке, которая равна  $1 + \beta^k + \beta^{2k} + \dots + \beta^{(\lambda-2)k} = (1 - \beta^{(\lambda-1)k}) / (1 - \beta^k) = 0 / (1 - \beta^k) = 0$  при  $\beta^k \neq 1$  (если  $\beta^k = 1$ , то  $\chi$  — главный характер и  $S(\lambda) = \lambda - 1$ ). Следовательно,  $S(\lambda + 1) = S(1)$ ,  $S(\lambda + 2) = S(2)$ ,  $\dots$ ,  $S(\lambda + n) = S(n)$ , откуда вытекает, что  $S(n)$  — *ограниченная функция*. Суммирование по частям дает

$$\begin{aligned} \sum_{n=1}^N \frac{\chi(n)}{n^s} &= \sum_{n=1}^N \frac{S(n) - S(n-1)}{n^s} = \sum_{n=1}^N \frac{S(n)}{n^s} - \sum_{n=2}^N \frac{S(n-1)}{n^s} = \\ &= \frac{S(N)}{N^s} + \sum_{n=1}^{N-1} S(n) \left[ \frac{1}{n^s} - \frac{1}{(n+1)^s} \right] \end{aligned}$$



поскольку  $S(0) = 0$ . При  $N \rightarrow \infty$  первый член стремится к 0, когда  $s > 0$ , поскольку числитель ограничен, а знаменатель стремится к  $\infty$ . Второй член — т. е. ряд — сходится при  $N \rightarrow \infty$ , в чем можно убедиться, сравнивая его с рядом

$$\sum_{n=1}^N \left[ \frac{1}{n^s} - \frac{1}{(n+1)^s} \right] = 1 - \frac{1}{2^s} + \frac{1}{2^s} - \frac{1}{3^s} + \dots = 1 - \frac{1}{(N+1)^s}$$

являющимся рядом с положительными членами, который сходится при  $s > 0$  и притом равномерно для  $s \geq \delta > 0$ . Это доказывает не только то, что ряд  $L(s, \chi) = \sum \chi(n) n^{-s}$  условно сходится при  $s > 0$ , но и то, что  $L(s, \chi)$  есть непрерывная и даже аналитическая функция переменной  $s$  при  $s > 0$  ( $\chi$  — неглавный характер).

Следовательно, для вычисления предела  $\lim L(s, \chi)$  при  $s \downarrow 1$  достаточно просуммировать условно сходящийся ряд  $\sum \chi(n)/n$ . Это можно сделать, комбинируя условно сходящиеся ряды<sup>1)</sup> вида

$$\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \dots$$

при значениях  $x = \alpha, \alpha^2, \dots, \alpha^{\lambda-1}$ , где, как и раньше,  $\alpha$  — примитивный корень  $\lambda$ -й степени из единицы. Например, пусть  $\lambda = 5$  и  $\chi$  — характер по модулю 5, определенный условием  $\chi(2) = -1$ . Тогда наша задача — просуммировать ряд

$$1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \frac{1}{11} - \dots$$

Метод сводится к тому, чтобы записать этот ряд как комбинацию рядов

$$\begin{aligned} \alpha + \frac{\alpha^2}{2} + \frac{\alpha^3}{3} + \frac{\alpha^4}{4} + \frac{\alpha^5}{5} + \dots &= \log \frac{1}{1-\alpha} \\ \alpha^2 + \frac{\alpha^4}{2} + \frac{\alpha^6}{3} + \frac{\alpha^8}{4} + \frac{\alpha^{10}}{5} + \dots &= \log \frac{1}{1-\alpha^2} \end{aligned}$$

<sup>1)</sup> Дирихле в своем выводе для описания функции  $-\log(1-x)$  воспользовался определенным интегралом, а не условно сходящимся рядом.

$$\alpha^3 + \frac{\alpha^6}{2} + \frac{\alpha^9}{3} + \frac{\alpha^{12}}{4} + \frac{\alpha^{15}}{5} + \dots = \log \frac{1}{1 - \alpha^3}$$

$$\alpha^4 + \frac{\alpha^8}{2} + \frac{\alpha^{12}}{3} + \frac{\alpha^{16}}{4} + \frac{\alpha^{20}}{5} + \dots = \log \frac{1}{1 - \alpha^4}$$

и (для удобства вычислений) расходящегося ряда

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots = \log \frac{1}{1 - 1}$$

Теперь нужно найти такой набор постоянных  $c_0, c_1, c_2, c_3, c_4$ , чтобы выполнялось равенство

$$1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \dots =$$

$$= c_0 \left( 1 + \frac{1}{2} + \dots \right) + c_1 \left( \alpha + \frac{\alpha^2}{2} + \dots \right) + c_2 \left( \alpha^2 + \frac{\alpha^4}{2} + \dots \right) +$$

$$+ c_3 \left( \alpha^3 + \frac{\alpha^6}{2} + \dots \right) + c_4 \left( \alpha^4 + \frac{\alpha^8}{2} + \dots \right).$$

Нам будет достаточно, если выполняются равенства

$$1 = c_0 + c_1 \alpha + c_2 \alpha^2 + c_3 \alpha^3 + c_4 \alpha^4$$

$$-1 = c_0 + c_1 \alpha^2 + c_2 \alpha^4 + c_3 \alpha^6 + c_4 \alpha^8$$

$$-1 = c_0 + c_1 \alpha^3 + c_2 \alpha^6 + c_3 \alpha^9 + c_4 \alpha^{12}$$

$$1 = c_0 + c_1 \alpha^4 + c_2 \alpha^8 + c_3 \alpha^{12} + c_4 \alpha^{16}$$

$$0 = c_0 + c_1 + c_2 + c_3 + c_4$$

(поскольку  $\alpha^5 = 1$ ). Суммирование этих равенств дает  $0 = 1 - 1 - 1 + 1 = 5c_0$ , ибо  $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^8 = \dots = 0$ . Аналогично, если первое равенство умножить на  $\alpha^{-1}$ , второе на  $\alpha^{-2}$  и т. д. и все пять равенств сложить, то получится  $\alpha^{-1} - \alpha^{-2} - \alpha^{-3} + \alpha^{-4} = 5c_1$ . Таким способом очень легко решается вся система 5 уравнений с 5 неизвестными,

и мы находим

$$c_0 = 0 \quad c_1 = \frac{\alpha^4 - \alpha^3 - \alpha^2 + \alpha}{5}$$

$$c_2 = \frac{\alpha^3 - \alpha - \alpha^4 + \alpha^2}{5} = -c_1 \quad c_3 = -c_1 \quad c_4 = c_1$$

Отсюда

$$1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \dots = c_1 \log \frac{1}{1-\alpha} - c_1 \log \frac{1}{1-\alpha^2} -$$

$$- c_1 \log \frac{1}{1-\alpha^3} + c_1 \log \frac{1}{1-\alpha^4}$$

где  $c_1 = (\alpha - \alpha^2 - \alpha^3 + \alpha^4)/5$ , а выражение  $\log (1 - \alpha^j)^{-1}$  поставлено вместо условно сходящегося ряда  $\alpha^j + \frac{1}{2}\alpha^{2j} + \frac{1}{3}\alpha^{3j} + \dots$ . Если бы удалось показать, что эти 4 условно сходящихся ряда действительно сходятся к числам  $\log (1 - \alpha^j)^{-1}$ , то отсюда вытекало бы, что число  $1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \dots$  равно числу, стоящему в правой части приведенного равенства.

Справедливость формулы

$$\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \dots \quad (1)$$

для всех комплексных чисел  $x$  в круге  $|x| \leq 1$ , кроме  $x = 1$ , может быть доказана суммированием по частям следующим образом. Пусть  $S(0) = 0$ ,  $S(n) = S(n-1) + x^n$ . Тогда  $S(n) = x + x^2 + \dots + x^n = (x - x^{n+1})/(1-x)$  и  $|S(n)|$  не превосходит  $2/|1-x|$ . Так как

$$\sum_{n=1}^N \frac{x^n}{n} = \sum_{n=1}^N \frac{S(n) - S(n-1)}{n} =$$

$$= \sum_{n=1}^N \frac{S(n)}{n} - \sum_{n=2}^N \frac{S(n-1)}{n} =$$

$$= \frac{S(N)}{N} + \sum_{n=1}^{N-1} S(n) \left[ \frac{1}{n} - \frac{1}{n+1} \right]$$

отсюда вытекает, что при  $N \rightarrow \infty$  ряд, стоящий в левой части, не только сходится, но сходится *равномерно* по  $x$  на множестве  $\{ |x| \leq 1, |x - 1| \geq \varepsilon \}$ ; достаточно сравнить его со сходящимся рядом

$$\sum \left[ (1/n) - (1/(n+1)) \right] = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \dots$$

Следовательно,  $\sum x^n/n$  определяет непрерывную функцию переменного  $x$  для  $|x| \leq 1, x \neq 1$ . Так как при  $|x| < 1$  эта функция есть  $\log(1/(1-x))$  (элементарный факт из комплексного анализа) и так как функция  $\log(1/(1-x))$  определена и непрерывна для  $|x| \leq 1, x \neq 1$ , искомая формула (1) установлена. Следовательно,

$$\begin{aligned} 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \dots &= \frac{\alpha - \alpha^2 - \alpha^3 + \alpha^4}{5} \times \\ &\times \left[ \log \frac{1}{1-\alpha} - \log \frac{1}{1-\alpha^2} - \log \frac{1}{1-\alpha^3} + \log \frac{1}{1-\alpha^4} \right] = \\ &= \frac{\theta_0 - \theta_1}{5} \left[ \log \frac{(1-\alpha^2)(1-\alpha^3)}{(1-\alpha)(1-\alpha^4)} + 2\pi ni \right] = \\ &= \frac{\theta_0 - \theta_1}{5} [\log(1-\theta_1) + 2\pi ni] \end{aligned}$$

где, как и раньше,  $\theta_0 = \alpha + \alpha^4$ ,  $\theta_1 = \alpha^2 + \alpha^3$ , так что  $(1-\alpha^2) \cdot (1-\alpha^3) = 2-\theta_1$ ,  $(1-\alpha)(1-\alpha^4) = 2-\theta_0$ ,  $(2-\theta_1)/(2-\theta_0) = (2-\theta_1)^2/(2-\theta_0)(2-\theta_1) = 1-\theta_1$ , как легко проверить вычислением. Заметим, что, поскольку  $\theta_0, \theta_1$  — вещественные числа, меньшие 1, целое число  $n$  должно быть нулем, когда используется вещественная ветвь логарифма  $\log(1-\theta_1)$ . Кроме того,  $(\theta_0 - \theta_1)^2 = 5$ . Меняя в случае надобности местами  $\theta_0$  и  $\theta_1$  (замена  $\alpha$  на  $\alpha^2$ ), мы можем считать, что  $\theta_0 - \theta_1 > 0$ . Тогда  $\theta_0 - \theta_1 = \sqrt{5}$ ,  $-1 - 2\theta_1 = \sqrt{5}$ ,  $1 - \theta_1 = (3 + \sqrt{5})/2$ , откуда следует окончательная формула

$$L(1, \chi) = \frac{\sqrt{5}}{5} \log \frac{3 + \sqrt{5}}{2}$$

в случае  $\lambda = 5, \chi(2) = -1$ .

Общая формула для  $L(1, \chi)$  может быть выведена точно такой же последовательностью шагов. Пусть  $\chi$  — неглавный характер

по модулю  $\lambda$  и  $\alpha$  — корень  $\lambda$ -й степени из единицы, причем  $\alpha \neq 1$ . Положим

$$\begin{aligned} 1 + \frac{\chi(2)}{2} + \frac{\chi(3)}{3} + \frac{\chi(4)}{4} + \dots = c_0 \left( 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots \right) + \\ + c_1 \left( \alpha + \frac{\alpha^2}{2} + \frac{\alpha^3}{3} + \dots \right) + \dots \\ \dots + c_{\lambda-1} \left( \alpha^{\lambda-1} + \frac{\alpha^{2\lambda-2}}{2} + \frac{\alpha^{3\lambda-3}}{3} + \dots \right). \end{aligned}$$

Для того чтобы выполнялось это равенство, достаточно потребовать от коэффициентов  $c_k$  выполнения условий

$$\chi(j) = \sum_{k=0}^{\lambda-1} c_k \alpha^{jk}.$$

Эту систему уравнений можно решить при помощи умножения  $j$ -го уравнения на  $\alpha^{-jv}$  с последующим суммированием. Находим

$$\sum_{j=1}^{\lambda-1} \chi(j) \alpha^{-jv} = \lambda c_v.$$

В частности,  $c_0 = 0$ , поскольку сумма значений характера  $\chi$  равна нулю ( $\chi$  не является главным характером). Следовательно,

$$L(1, \chi) = \sum_{v=1}^{\lambda-1} c_v \log \frac{1}{1 - \alpha^v}, \quad (2)$$

где

$$c_v = \frac{1}{\lambda} \sum_{j=1}^{\lambda-1} \chi(j) \alpha^{-jv}. \quad (3)$$

Выражение для  $L(1, \chi)$ , даваемое равенствами (2) и (3), можно еще упростить следующим образом. Пусть  $\gamma$  — примитивный корень по модулю  $\lambda$ , и пусть  $\sigma: \alpha \mapsto \alpha^\gamma$  — соответствующее сопряжение для круговых целых. Тогда в (2) естественно записать  $\lambda - 1$  членов со степенями элемента  $\alpha$  в порядке  $\alpha, \sigma\alpha, \sigma^2\alpha, \dots$  вместо порядка  $\alpha, \alpha^2, \alpha^3, \dots$ . (Замечаем, что  $c_0 = 0$ .) После этого формула (2) приобретает вид

$$(L(1, \chi)) = \sum_{k=0}^{\lambda-2} b_k \log \frac{1}{1 - \sigma^k \alpha},$$

где  $b_k$  представляют собой прежние  $c_v$ , но поставленные в другом порядке. Действительно,  $b_k = c_v$ , где  $v \equiv \gamma^k \pmod{\lambda}$ , откуда

$$b_k = c_v = \frac{1}{\lambda} \sum_{j=1}^{\lambda-1} \chi(j) \sigma^k \alpha^{-j} = \sigma^k (b_0)$$

(сопряжение  $\sigma$  очевидным образом применяется к линейной комбинации степеней  $\alpha$  с комплексными коэффициентами). Пусть  $\rho$  обозначает  $\chi(\gamma)$ . Тогда

$$\begin{aligned} b_0 &= \frac{1}{\lambda} [\chi(1)\alpha^{-1} + \chi(2)\alpha^{-2} + \chi(3)\alpha^{-3} + \dots] = \\ &= \frac{1}{\lambda} [\alpha^{-1} + \chi(\gamma)\alpha^{-\gamma} + \dots + \chi(\gamma^j)\sigma^j\alpha^{-1} + \dots] = \\ &= \frac{1}{\lambda} [\sigma^\mu\alpha + \rho\sigma^{\mu+1}\alpha + \dots + \rho^j\sigma^{\mu+j}\alpha + \dots] = \\ &= \frac{\rho^{-\mu}}{\lambda} [\alpha + \rho\sigma\alpha + \dots + \rho^k\sigma^k\alpha + \dots], \end{aligned}$$

где  $\mu = (\lambda - 1)/2$  (см. упр. 3) и где каждая сумма содержит  $\lambda - 1$  членов. Следовательно,

$$\begin{aligned} b_k &= \sigma^k b_0 = \frac{\rho^{-\mu}}{\lambda} [\sigma^k\alpha + \rho\sigma^{k+1}\alpha + \dots] = \\ &= \frac{\rho^{-\mu-k}}{\lambda} [\rho^k\sigma^k\alpha + \rho^{k+1}\sigma^{k+1}\alpha + \dots] = \rho^{-k} b_0 \end{aligned}$$

и

$$L(1, \chi) = b_0 \sum_{k=0}^{\lambda-2} \rho^{-k} \log \frac{1}{1 - \sigma^k \alpha}.$$

Сомножитель  $\rho^{-\mu}$ , который участвует в выражении для  $b_0$ , равен  $\pm 1$ , поскольку  $(\rho^\mu)^2 = \rho^{\lambda-1} = \chi(\gamma^{\lambda-1}) = \chi(1) = 1$ . Кроме того,  $\rho = \beta^j$ , где  $\beta$  — некоторый примитивный корень  $(\lambda - 1)$ -й степени из единицы, и  $\beta^\mu = -1$ . Значит,  $\rho^{-\mu} = 1$ , если  $j$  четно, и  $\rho^{-\mu} = -1$ , если  $j$  нечетно. Пусть  $\chi_j$  обозначает характер по модулю  $\lambda$ , для которого  $\chi(\gamma) = \beta^j$ . Тогда полученные ранее формулы дают

$$L(1, \chi_j) = (-1)^j m_j \sum_{k=0}^{\lambda-2} \beta^{-jk} \log \frac{1}{1 - \sigma^k \alpha}, \quad (4)$$



где

$$m_j = \frac{1}{\lambda} \sum_{k=0}^{\lambda-2} \beta^{jk} \sigma^k \alpha. \quad (5)$$

Когда  $j$  четно, два члена

$$\beta^{-jk} \log \frac{1}{1 - \sigma^k \alpha} + \beta^{-j(k+\mu)} \log \frac{1}{1 - \sigma^{k+\mu} \alpha}$$

в формуле для  $L(1, \chi_j)$  можно объединить, и, поскольку  $\beta^{-j\mu} = 1$ , а  $\sigma^{k+\mu} \alpha$  комплексно сопряжено с  $\sigma^k \alpha$ , мы получаем

$$\beta^{-jk} 2 \operatorname{Re} \log \frac{1}{1 - \sigma^k \alpha} = -2\beta^{-jk} \log |1 - \sigma^k \alpha|.$$

Следовательно,

$$L(1, \chi_{2\nu}) = -2m_{2\nu} \sum_{k=0}^{\mu-1} \beta^{-2\nu k} \log |1 - \sigma^k \alpha|. \quad (6)$$

С другой стороны, когда  $j$  нечетно, вещественные части уничтожаются и

$$L(1, \chi_{2\nu+1}) = -m_{2\nu+1} \sum_{k=0}^{\lambda-2} \beta^{-(2\nu+1)k} i \operatorname{Im} \log \frac{1}{1 - \sigma^k \alpha},$$

где мнимая часть функции  $\log(1-x)^{-1}$  определена на окружности  $|x| = 1$  таким образом, чтобы она была непрерывным продолжением ветви, принимающей внутри круга значение нуль для вещественных  $x$ . Если  $x$  лежит внутри этого круга, то  $\operatorname{Re}(1-x)^{-1}$ , как легко видеть, больше  $1/2$ , откуда следует, что мнимая часть ее логарифма заключена между  $-\pi/2$  и  $\pi/2$ . Значит, это же верно и для  $\operatorname{Im} \log(1-x)^{-1}$  при  $|x| = 1$  ( $x \neq 1$ ). Далее, если  $\sigma^k \alpha = e^{i\theta}$ , то

$$\frac{1}{1 - \sigma^k \alpha} = \frac{1}{1 - e^{i\theta}} = \frac{e^{-i\theta/2}}{e^{-i\theta/2} - e^{i\theta/2}} = \frac{e^{-i\theta/2}}{-2i \sin \frac{\theta}{2}} = \frac{e^{i(\pi-\theta)/2}}{2 \sin \frac{\theta}{2}},$$

$$\log \frac{1}{1 - \sigma^k \alpha} = -\log \left( 2 \sin \frac{\theta}{2} \right) + \frac{i}{2} (\pi - \theta), \quad (7)$$

где  $(\pi - \theta)/2$  лежит между  $-\pi/2$  и  $\pi/2$ , так что  $\theta$  лежит между  $0$  и  $2\pi$ . Если выбрать  $\alpha$  равным  $e^{2\pi i/\lambda}$ , то  $\sigma^k \alpha$  окажется равным  $e^{2\pi i \gamma^k/\lambda}$  в степени  $\gamma^k$ , и соответствующее  $\theta$  равно  $2\pi \gamma^k/\lambda$ , редуцированному по модулю  $2\pi$ , т. е.  $\theta$  лежит между  $0$  и  $2\pi$ . Значит,  $\theta = 2\pi \gamma_k/\lambda$ , где целое число  $\gamma_k$  определено условиями  $0 < \gamma_k < \lambda$ ,  $\gamma_k \equiv \gamma^k \pmod{\lambda}$ . Таким образом, при нечетном  $j$  формула прини-

мает вид

$$\begin{aligned} L(1, \chi_{2v+1}) &= -m_{2v+1} \sum_{k=0}^{\lambda-2} \beta^{-(2v+1)k} i \left( \frac{\pi - \theta}{2} \right) = \\ &= \text{const} \sum_{k=0}^{\lambda-2} \beta^{-(2v+1)k} - m_{2v+1} \sum_{k=0}^{\lambda-2} \beta^{-(2v+1)k} i \left( -\frac{2\pi\gamma_k}{2\lambda} \right), \end{aligned}$$

и окончательно

$$L(1, \chi_{2v+1}) = \frac{i\pi m_{2v+1}}{\lambda} \sum_{k=0}^{\lambda-2} \gamma_k \beta^{-(2v+1)k}, \quad (8)$$

где  $m_{2v+1}$  определено формулой (5),  $\chi_{2v+1}$  — характер, определенный условием  $\chi_{2v+1}(\gamma) = \beta^{2v+1}$ , и целые числа  $\gamma_k$  определены условиями  $0 < \gamma_k < \lambda$ ,  $\gamma_k \equiv \gamma^k \pmod{\lambda}$ .

## Упражнения

1. Формула для  $L(1, \chi)$  в случае  $\lambda = 5$ ,  $\chi(2) = -1$  была получена в тексте при предположении  $\theta_0 - \theta_1 > 0$ . Если  $\theta_0 - \theta_1 < 0$ , то получается на вид совсем другая формула. Покажите, что обе формулы представляют одно и то же число.

2. В случае  $\lambda = 7$ ,  $\chi(3) = -1$  найдите  $L(1, \chi)$  с тремя значащими цифрами.

3. Покажите, что если  $\mu = (\lambda - 1)/2$ , то  $\sigma^\mu \alpha = \alpha^{-1}$ .

4. Найдите  $L(1, \chi)$  явно для всех неглавных характеров  $\chi$  во всех случаях при  $\lambda = 3, 5, 7$ .

## 6.6. Предел правой части

Пусть  $\lambda$  — данное простое число,  $\gamma$  — примитивный корень по модулю  $\lambda$ ,  $\beta$  — примитивный корень  $(\lambda - 1)$ -й степени из единицы (т. е.  $\beta^{\lambda-1} = 1$ ,  $\beta^j \neq 1$  при  $0 < j < \lambda - 1$ ), и пусть  $\chi_j$  обозначает характер по модулю  $\lambda$ , определенный условием  $\chi_j(\gamma) = \beta^j$ . Тогда  $\chi_0, \chi_1, \dots, \chi_{\lambda-2}$  — полный список характеров по модулю  $\lambda$ , и, как показано в § 6.4,

$$\lim_{s \downarrow 1} (s-1) \prod \left( 1 - \frac{1}{N(P)^s} \right)^{-1} = L(1, \chi_1) L(1, \chi_2) \dots L(1, \chi_{\lambda-2}), \quad (1)$$

где в левой части произведение берется по всем простым дивизорам  $P$  круговых целых, построенных при помощи примитивного корня  $\lambda$ -й степени из единицы. В § 6.5 было показано, что каждый сомножитель  $L(1, \chi_j)$  правой части может быть записан в явном виде. Именно, если

$$m_j = \frac{1}{\lambda} \sum_{k=0}^{\lambda-2} \beta^{jk} \sigma^k \alpha \quad (2)$$

(как обычно,  $\sigma: \alpha \mapsto \alpha^\gamma$  для выбранного примитивного корня  $\gamma$  по модулю  $\lambda$ ), то

$$L(1, \chi_{2\nu}) = -2m_{2\nu} \sum_{k=0}^{\mu-1} \beta^{-2\nu k} \log |1 - \sigma^k \alpha|$$

(где  $\mu = (\lambda - 1)/2$ ) и

$$L(1, \chi_{2\nu+1}) = \frac{i\pi}{\lambda} m_{2\nu+1} \sum_{k=0}^{\lambda-2} \gamma_k \beta^{-(2\nu+1)k};$$

при этом в определении чисел  $m_{2\nu+1}$  используется значение  $\alpha = e^{2\pi i/\lambda}$ , а целые числа  $\gamma_k$  определяются условиями  $0 < \gamma_k < \lambda$ ,  $\gamma_k \equiv \gamma^k \pmod{\lambda}$ .

Пусть

$$C_\nu = \sum_{k=0}^{\mu-1} \beta^{-2\nu k} \log |1 - \sigma^k \alpha|,$$

и пусть через  $\varphi(X)$  обозначен полином

$$\varphi(X) = \sum_{k=0}^{\lambda-2} \gamma_k X^k.$$

Тогда, поскольку  $\beta^{-1} = \beta^{\lambda-2}$ ,  $\beta^{-3} = \beta^{\lambda-4}$ , ..., для предела в (1) получается следующее выражение:

$$(-2)^{\mu-1} \left( \frac{i\pi}{\lambda} \right)^\mu m_1 m_2 \dots m_{\lambda-2} C_1 C_2 \dots C_{\mu-1} \varphi(\beta) \varphi(\beta^3) \dots \varphi(\beta^{\lambda-2}).$$

Вторая часть вывода формулы числа классов состоит в вычислении предела  $(s-1) \sum N(A)^{-s}$  при  $s \downarrow 1$ . Прежде чем приступить к ней, полезно заметить, что простым следствием полученных формул является *необращение в нуль* величин  $L(1, \chi)$  для неглавных характеров  $\chi$ . Ближайший параграф посвящен доказательству того, что  $L(1, \chi) \neq 0$ , а в следующем за ним будет продолжен вывод формулы числа классов.

## 6.7. Необращение в нуль $L$ -рядов

Основной трудностью в доказательстве теоремы Дирихле о простых числах в арифметической прогрессии является доказательство того, что если  $\chi$  — неглавный характер по модулю  $\lambda$  (в теореме Дирихле число  $\lambda$  не обязательно простое), то  $L(1, \chi) \neq 0$ . По различным причинам тот же факт требуется при выводе формулы Куммера числа классов, но в этом случае можно ограничиться самым легким случаем, когда  $\lambda$  — простое. В этом случае утверждение  $L(1, \chi) \neq 0$  допускает следующее простое доказательство.

Пусть  $\chi$  — неглавный характер по модулю  $\lambda$ . Нужно показать, что  $L(1, \chi) \neq 0$ . Пусть  $\rho = \chi(\gamma)$ , где  $\gamma$  — примитивный корень по модулю  $\lambda$ . По предположению,  $\rho \neq 1$ . Если  $\rho \neq -1$ , то  $\rho$  не вещественно и  $\overline{\chi(\gamma)} = \bar{\rho} \neq \chi(\gamma)$ . Таким образом, в случае  $\rho \neq -1$  характеры  $\chi$  и  $\bar{\chi}$  (комплексно сопряженный характеру  $\chi$ ) различны. Так как  $L(1, \bar{\chi}) = \sum \bar{\chi}(n)/n = \overline{L(1, \chi)}$ , то отсюда следует, что в этом случае из  $L(1, \chi) = 0$  вытекало бы существование *двух различных* неглавных характеров  $\chi$ , для которых  $L(1, \chi) = 0$ . Значит, теорема будет доказана, если мы покажем, что  $L(1, \chi) = 0$  не более чем для одного неглавного характера  $\chi$  и что  $L(1, \chi) \neq 0$  для конкретного характера, определенного условием  $\chi(\gamma) = -1$ .

Напомним, что

$$\prod \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \zeta(s) L(s, \chi_1) L(s, \chi_2) \dots L(s, \chi_{\lambda-2}),$$

где  $\chi_1, \chi_2, \dots, \chi_{\lambda-2}$  — неглавные характеры по модулю  $\lambda$ . Кроме того, функция  $L(s, \chi_j)$  есть предел равномерно сходящейся при  $s \geq \varepsilon > 0$  последовательности аналитических функций и поэтому является аналитической, т. е. ее можно разложить в степенной ряд в окрестности любого  $s$ . В частности, она дифференцируема при  $s = 1$ , и если  $L(1, \chi_j) = 0$ , то существует предел

$$\lim_{s \rightarrow 1} \frac{L(s, \chi_j)}{s-1} = L'(1, \chi_j).$$

Значит, если  $L(1, \chi_j) = 0$  для двух различных значений  $j$ , то

$$\begin{aligned} \lim_{s \downarrow 1} \prod \left(1 - \frac{1}{N(P)^s}\right)^{-1} &= \\ &= \lim_{s \downarrow 1} \left[ \frac{L(s, \chi_1) \dots L(s, \chi_{\lambda-2})}{(s-1)^2} \right] \cdot [s-1] \cdot [(s-1)\zeta(s)] = \\ &= \text{конечная величина} \cdot 0 \cdot 1 = 0, \end{aligned}$$

что невозможно, поскольку произведение в левой части не менее 1 для каждого  $s > 1$  и, следовательно, при  $s \downarrow 1$  не может иметь пределом 0. Таким образом, равенство  $L(1, \chi_j) = 0$  выполняется не более чем для одного неглавного характера, а значит, разве лишь для характера  $\chi$ , для которого  $\chi(\gamma) = -1$  и который является характером  $\chi_\mu$  (где  $\mu = (\lambda - 1)/2$ ). Для этого характера утверждение  $L(1, \chi_\mu) \neq 0$  можно доказать, используя явную формулу для этого значения.

Так как  $\chi_\mu(\gamma) = \rho = -1$ , то формулы (4), (5) из § 6.5 дают

$$\begin{aligned} L(1, \chi_\mu) &= \pm m_\mu \sum_{k=0}^{\lambda-2} (-1)^k \log \frac{1}{1-\sigma^k \alpha} = \\ &= \pm \frac{1}{\lambda} (\alpha - \sigma\alpha + \sigma^2\alpha - \dots) \left( \log \frac{1}{1-\alpha} - \log \frac{1}{1-\sigma\alpha} + \right. \\ &\quad \left. + \log \frac{1}{1-\sigma^2\alpha} - \dots \right) = \\ &= \pm \frac{\theta_0 - \theta_1}{\lambda} \left[ \log \frac{(1-\sigma\alpha)(1-\sigma^3\alpha)\dots}{(1-\alpha)(1-\sigma^2\alpha)\dots} + 2\pi i n \right], \end{aligned}$$

где  $\theta_0$  — период длины  $\mu$ , содержащий  $\alpha$ ,  $\theta_1 = \sigma\theta_0$  и  $n$  — целое число. Первый сомножитель может быть нулем, только если  $\theta_0 = \theta_1$ . Это невозможно, поскольку из  $\theta_0 = \theta_1 = \sigma\theta_0$  вытекало бы, что  $\theta_0$  — обычное целое число и в то же время  $0 = 1 + \theta_0 + \dots + \theta_1 = 1 + 2\theta_0$ , что невозможно. Второй сомножитель может быть нулем только тогда, когда комплексное число, логарифмом которого оно является, есть 1, т. е. только тогда, когда числитель  $\prod (1 - \sigma^{2v+1}\alpha)$  равен знаменателю  $\prod (1 - \sigma^{2v}\alpha)$ . Но это невозможно, поскольку их общее значение было бы целым числом (ибо оно инвариантно относительно  $\sigma$ ), квадрат которого равен  $\prod (1 - \sigma^v\alpha) = N(1 - \alpha) = \lambda$ , вопреки предположению, что число  $\lambda$  простое. Это завершает доказательство того, что  $L(1, \chi) \neq 0$  для всех неглавных характеров  $\chi$  по модулю  $\lambda$ .

## 6.8. Преобразование левой части

Вторая половина вывода формулы числа классов требует вычисления левой части формулы эйлерова произведения

$$\sum \frac{1}{N(A)^s} = \prod \left( 1 - \frac{1}{N(P)^s} \right)^{-1}.$$

Точнее, нужно оценить, как растет левая часть при  $s \downarrow 1$ . Для этого нужно очевидным образом модифицировать тот прием, которым пользовался Дирихле при выводе своей формулы числа классов, и *разбить сумму по всем дивизорам на суммы по классам дивизоров, а затем доказать, что в пределе при  $s \downarrow 1$  все эти суммы равны*. Итак, пусть  $A_1, A_2, \dots, A_h$  — система представителей дивизоров (см. § 5.3); перепишем нашу сумму так:

$$\sum N(A)^{-s} = \sum_{A \sim A_1} N(A)^{-s} + \sum_{A \sim A_2} N(A)^{-s} + \dots + \sum_{A \sim A_h} N(A)^{-s}.$$

(Перестановка в сумме оправдана абсолютной сходимостью.) Как подсказывает работа Дирихле, — и это сравнительно легко дока-

зять — дело сводится к тому что выписанные слагаемые одинаково стремятся к  $\infty$  при  $s \downarrow 1$ , точнее, предел

$$\lim_{s \downarrow 1} (s-1) \sum_{A \sim A_j} N(A)^{-s}$$

существует и одинаков для всех  $j$ . Таким образом, если  $L$  обозначает этот общий предел, то

$$\lim_{s \downarrow 1} (s-1) \sum N(A)^{-s} = hL.$$

Так как этот предел в предшествующих параграфах был подсчитан другим способом, не использующим величину  $h$ , то чтобы прийти к искомой формуле для  $h$ , нам нужно только найти  $L$ .

Основная часть предстоящей нам работы состоит в вычислении предела  $L$ . Ее можно проделать, вычисляя его для какого-нибудь одного класса эквивалентности дивизоров. Естественно воспользоваться *главным* классом, т. е. вычислить предел

$$\lim_{s \downarrow 1} (s-1) \sum_{A \sim I} N(A)^{-s} = L.$$

Условие  $A \sim I$  означает, что  $A$  — дивизор некоторого кругового целого  $g(\alpha)$ , поэтому сумму под знаком предела можно записать в виде суммы по круговым целым  $\sum N g(\alpha)^{-s}$ , если только мы сможем придумать правило выбора среди всех круговых целых, имеющих данный дивизор  $A$ , одного конкретного  $g(\alpha)$  с таким дивизором  $A$ . Найти такое правило выбора — это означает, по существу, изучить структуру *единиц* этой арифметики. Действительно, если  $g(\alpha)$  — любое круговое целое, то множество всех круговых целых с тем же дивизором, что и  $g(\alpha)$ , есть  $\{e(\alpha) g(\alpha) : e(\alpha) \text{ — единица}\}$ , и задача заключается в том, чтобы выбрать некоторый конкретный элемент в этом множестве  $\{e(\alpha) g(\alpha)\}$ .

Коль скоро правило выбора найдено, искомый предел

$$L = \lim_{s \downarrow 1} (s-1) \sum_{\substack{g(\alpha) \text{ выбрано} \\ \text{по правилу}}} N g(\alpha)^{-s}$$

сравнительно легко вычислить, если доказать, что *сумма* отличается на ограниченную величину от аналогичного *интеграла* при  $s \downarrow 1$ . Тогда искомый предел можно представить как интеграл, который можно подсчитать с помощью техники интегрального исчисления. Этот последний шаг аналогичен вычислению предела

$$\lim_{s \downarrow 1} (s-1) \sum_{n=N}^{\infty} n^{-s}$$



с использованием того, что при  $s \downarrow 1$  сумма отличается на ограниченную величину от интеграла  $\int_c^\infty x^{-s} dx$  (ибо, если исключить конечные отрезки, на которых и сумма, и интеграл ограничены, слагаемое в сумме отличается от значения подынтегральной функции на величину порядка  $n^{-s} - (n+1)^{-s} \sim (-s) n^{-s-1}$ , а сумма таких величин конечна при  $s \geq 1$ ). Отсюда

$$\lim_{s \downarrow 1} (s-1) \sum_{n=N}^{\infty} n^{-s} = \lim_{s \downarrow 1} (s-1) \left[ \int_c^\infty x^{-s} dx + \right. \\ \left. + \text{ограниченная величина} \right] = \lim_{s \downarrow 1} (s-1) \frac{c^{1-s}}{s-1} + 0 = c^0 = 1.$$

Итак, перечислим по порядку, чем мы будем заниматься в нескольких ближайших параграфах. Вначале будут изучены круговые единицы, чтобы вывести правило выбора для выделения по любому главному дивизору  $A$  кругового целого  $g(\alpha)$  с этим дивизором. (На самом деле наше правило выбора будет осуществлять чуть-чуть меньше этого.) Затем будет вычислен предел  $L$  для главных дивизоров путем сравнения суммы с интегралом. Далее, будет доказано, что предел  $L$  для других классов дивизоров такой же, как и для главного класса. Наконец,  $hL$  будет приравнено другому выражению того же предела, полученному в предшествующем параграфе, и формула для  $h$  будет выведена

## 6.9. Единицы: несколько первых случаев

По причинам, объясненным в предыдущем параграфе, вычисление суммы слагаемых  $N(A)^{-s}$  по всем главным дивизорам  $A$  тесно связано со знанием круговых единиц. В этом параграфе изучаются единицы в случаях  $\lambda = 3, 5, 7, 11$  и  $17$ . Общий случай, который является простым обобщением этих случаев, излагается в следующем параграфе.

В § 5.5 было показано, что частное от деления круговой единицы на комплексно сопряженную с ней, т.е.  $e(\alpha)/e(\alpha^{-1})$ , есть степень числа  $\alpha$ . В этом параграфе удобно переформулировать это утверждение следующим образом: *каждая круговая единица есть степень числа  $\alpha$ , умноженная на вещественную единицу*. Чтобы доказать утверждение в этой форме, заметим, что в равенстве  $e(\alpha)/e(\alpha^{-1}) = \alpha^k$  можно считать, не нарушая общности, число  $k$  четным, ибо если  $k$  нечетно, то его можно заменить на  $k + \lambda$ . Тогда, обозначив  $k = 2j$ , мы можем записать равенство в виде  $e(\alpha) \alpha^{-j} = e(\alpha^{-1}) \alpha^j$ . Значит, для единицы  $E(\alpha) = e(\alpha) \alpha^{-j}$  имеет место равенство  $E(\alpha) = E(\alpha^{-1})$ , т.е. единица  $E(\alpha)$  являет-

ся вещественной. Так как  $e(\alpha) = \alpha^j E(\alpha)$ , то это доказывает наше утверждение.

Таким образом, чтобы найти все единицы, достаточно найти все *вещественные* единицы. Сначала рассмотрим случай  $\lambda = 3$ . В этом случае круговое целое тогда и только тогда вещественно, когда оно инвариантно относительно единственного сопряжения  $\alpha \mapsto \alpha^2$ , а это верно в том и только том случае, когда оно является обычным целым числом. Норма обычного целого числа  $n$  есть просто его квадрат  $n^2$ . Таким образом, единственные вещественные единицы — это  $\pm 1$ , и всего имеется *точно шесть единиц*:  $\pm 1, \pm \alpha, \pm \alpha^2$ . В этом случае каждый главный дивизор  $A$  является дивизором точно шести круговых целых  $g(\alpha)$ , и можно написать

$$\sum_{A \text{ главный}} N(A)^{-s} = \frac{1}{6} \sum N g(\alpha)^{-s} \quad (\lambda = 3),$$

где в правой части стоит сумма по всем круговым целым.

Однако во всех остальных случаях число круговых единиц бесконечно. Рассмотрим следующий случай  $\lambda = 5$ . Здесь элемент  $a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$  веществен тогда и только тогда, когда он инвариантен относительно  $\alpha \mapsto \alpha^4$ , а это верно в том и только том случае, когда его можно записать в виде  $a\theta_0 + b\theta_1$ , где, как обычно,  $\theta_0 = \alpha + \alpha^4$ ,  $\theta_1 = \alpha^2 + \alpha^3$ . Норма элемента  $a\theta_0 + b\theta_1$  есть квадрат числа  $(a\theta_0 + b\theta_1)(a\theta_1 + b\theta_0) = (a^2 + b^2)\theta_0\theta_1 + ab(\theta_0^2 + \theta_1^2) = (a^2 + b^2)^{1/4}[(\theta_0 + \theta_1)^2 - (\theta_0 - \theta_1)^2] + ab^{1/2}[(\theta_0 + \theta_1)^2 + (\theta_0 - \theta_1)^2] = (a^2 + b^2)^{1/4}[1 - 5] + ab^{1/2}[1 + 5] = -a^2 - b^2 + 3ab$ . Таким образом, единица  $a\theta_0 + b\theta_1$  тогда и только тогда вещественна, когда  $a$  и  $b$  — такие целые числа, что  $a^2 + b^2 - 3ab = \pm 1$ . В частности,  $\theta_0$  — вещественная единица. Значит, элементы  $\pm 1, \pm \theta_0, \pm \theta_0^2 = \pm(2 + \theta_1), \pm \theta_0^3 = \pm(-1 + 2\theta_0), \dots$ , а также их сопряженные являются вещественными единицами. Единицы в этом списке попарно различны, и список содержит все вещественные единицы; это можно доказать разными способами (см. упр. 1), например приспособив к этому случаю рассуждение, которое будет проведено дальше в случае  $\lambda = 7$ .

Однако даже при помощи столь полного описания единиц еще не совсем очевидно, как сосчитать сумму  $\sum N(A)^{-s}$  по всем главным дивизорам  $A$ . Для этой цели полезно представить себе круговые целые как точки комплексной плоскости, положив, например,  $\alpha = e^{2\pi i/5}$ . Тогда имеется десять единиц  $\pm \alpha^j$  на единичной окружности, десять единиц  $\pm \alpha^j \theta_0$  на окружности радиуса  $|\theta_0| = 2 \cos(2\pi/5)$ , десять единиц  $\pm \alpha^j \theta_0^2$  на окружности радиуса  $2^2 \cos^2(2\pi/5)$  и т. д. Отсюда геометрически ясно, что для каждого данного отличного от нуля кругового целого  $g(\alpha)$  имеется такая единица  $e(\alpha)$ , что  $1 \leq |e(\alpha)g(\alpha)| < |\theta_0|$ , где  $|\cdot|$  обозначает

модуль комплексного числа; для этого нужно лишь выбрать такое  $n$ , чтобы  $|\theta_0|^n \leq |g(\alpha)| < |\theta_0|^{n+1}$ , и положить  $e(\alpha) = \theta_0^{-n}$ . Если  $e_1(\alpha)$  и  $e_2(\alpha)$  — две единицы, обладающие этим свойством, то  $|\theta_0|^{-1} < |e_1(\alpha)^{-1} g(\alpha)^{-1} e_2(\alpha) g(\alpha)| < |\theta_0|$ , т. е.  $|\theta_0|^{-1} < |e_1(\alpha)^{-1} e_2(\alpha)| < |\theta_0|$ . Поскольку каждая единица имеет вид  $\pm \theta_0^n \alpha^j$ , отсюда следует, что  $e_1(\alpha)^{-1} e_2(\alpha)$  может быть одной из десяти единиц  $\pm 1, \pm \alpha, \pm \alpha^2, \pm \alpha^3, \pm \alpha^4$ . Значит, имеется точно десять единиц  $e(\alpha)$ , для которых выполняется условие  $1 \leq |e(\alpha) g(\alpha)| < |\theta_0|$ . Иначе говоря, для данного ненулевого кругового целого  $g(\alpha)$  имеется точно десять круговых целых  $h(\alpha)$ , имеющих тот же дивизор, что и  $g(\alpha)$ , и лежащих в кольце  $1 \leq |h(\alpha)| < |\theta_0|$ . Значит, формула

$$\sum_{A \text{ главный}} N(A)^{-s} = \frac{1}{10} \sum_{1 \leq |g(\alpha)| < |\theta_0|} N g(\alpha)^{-s}$$

сводит сумму по всем главным дивизорам к сумме по круговым целым.

В следующем случае  $\lambda = 7$  имеется 14 единиц вида  $\pm \alpha^j$ . Если двигаться намеченным путем, то сначала нужно изучить вещественные единицы. Круговое целое при  $\lambda = 7$  вещественно тогда и только тогда, когда оно имеет вид  $a\eta_0 + b\eta_1 + c\eta_2$ , где  $\eta_0 = \alpha + \alpha^{-1}$ ,  $\eta_1 = \alpha^3 + \alpha^{-3}$ ,  $\eta_2 = \alpha^2 + \alpha^{-2}$  — периоды длины 2. Не очень длинное вычисление (упр. 2) показывает, что норма элемента  $a\eta_0 + b\eta_1 + c\eta_2$  равна

$$[(a + b + c)^3 - 7(a^2b + b^2c + c^2a + abc)]^2.$$

Значит, вещественные единицы — это те элементы  $a\eta_0 + b\eta_1 + c\eta_2$ , для которых  $(a + b + c)^3 - 7(a^2b + b^2c + c^2a + abc) = \pm 1$ . Далее наша задача заключается в том, чтобы найти все тройки  $a, b, c$  целых чисел, для которых имеет место это равенство. Эта задача не так уж проста, но она может быть решена следующим образом.

Заметим сначала, что  $\eta_0$  — единица. Это ясно, например, из того, что  $\eta_0 = \alpha + \alpha^4 = \alpha^{-1}(\alpha^2 + 1) = \alpha^{-1}(\alpha^4 - 1)/(\alpha^2 - 1)$ , поскольку  $\alpha^4 - 1$  и  $\alpha^2 - 1$ , имея один и тот же дивизор  $(\alpha - 1)$ , отличаются на сомножитель, являющийся единицей. Значит,  $\eta_1$  и  $\eta_2$  также являются единицами, и выражение  $\pm \eta_0^l \eta_1^m \eta_2^n$  ( $l, m, n$  — целые числа) есть формула, дающая большое число вещественных единиц. Так как  $\eta_0 \eta_1 \eta_2 = 1$  (это легко подсчитать), то каждая единица вида  $\pm \eta_0^l \eta_1^m \eta_2^n$  может быть записана в виде  $\pm \eta_0^r \eta_1^s$  ( $r, s$  — целые). Далее естественно возникают вопросы, различны ли вещественные единицы  $\pm \eta_0^r \eta_1^s$  и охватывают ли они все вещественные единицы.

То, что единицы  $\pm \eta_0^r \eta_1^s$  все различны, можно доказать следующим образом. Равенство  $\pm \eta_0^r \eta_1^s = \pm \eta_0^R \eta_1^S$  равносильно равенству  $\pm \eta_0^{r-R} \eta_1^{s-S} = 1$ , поэтому нам нужно показать, что равенство

$\eta_0^r \eta_1^s = \pm 1$  возможно лишь при  $r = 0, s = 0$ . Будем рассматривать круговые целые как комплексные числа, положив  $\alpha = e^{2\pi i/7}$ . Тогда значение  $\log |g(\alpha)|$  определено для всех отличных от нуля круговых целых  $g(\alpha)$ , и из  $\eta_0^r \eta_1^s = \pm 1$  вытекает следующее соотношение между  $r$  и  $s$ :

$$r \log |\eta_0| + s \log |\eta_1| = 0.$$

Применяя к этому соотношению сопряжение, определяемое заменой  $\sigma: \alpha \mapsto \alpha^3$ , можно получить другое соотношение между  $r$  и  $s$ :

$$r \log |\eta_1| + s \log |\eta_2| = 0.$$

Для того чтобы утверждать, что обязательно  $r = s = 0$ , достаточно доказать, что определитель из коэффициентов

$$\begin{vmatrix} \log |\eta_0| & \log |\eta_1| \\ \log |\eta_1| & \log |\eta_2| \end{vmatrix}$$

отличен от нуля. Но это непосредственно ясно, поскольку  $\log |\eta_0| = \log (2 \cos (2\pi/7)) > 0$ ,  $\log |\eta_1| = \log (-2 \cos (6\pi/7)) > 0$ ,  $\log |\eta_2| = -\log |\eta_0| - \log |\eta_1| < 0$ . Следовательно, вещественные единицы  $\pm \eta_0^r \eta_1^s$  все различны.

Пусть теперь  $E(\alpha) = a\eta_0 + b\eta_1 + c\eta_2$  — данная вещественная единица. Задача состоит в том, чтобы найти, если это возможно, такую пару целых чисел  $(r, s)$ , что  $\eta_0^r \eta_1^s = \pm E(\alpha)$ . Использование функции  $\log |g(\alpha)|$  и сопряженной с ней  $\log |g(\alpha^3)|$ , как и раньше, показывает, что искомое соотношение дает

$$r \log |\eta_0| + s \log |\eta_1| = \log |E(\alpha)|, \tag{1}$$

$$r \log |\eta_1| + s \log |\eta_2| = \log |E(\alpha^3)|.$$

Так как матрица коэффициентов левых частей имеет ненулевой определитель, эта система уравнений имеет решение с *вещественными*  $r$  и  $s$  при заданной единице  $E(\alpha)$ . Достаточно показать, что  $r$  и  $s$  обязательно должны быть *целыми числами*, поскольку тогда  $E(\alpha) \eta_0^{-r} \eta_1^{-s}$  окажется вещественной единицей, логарифм модуля которой равен 0, т. е.  $E(\alpha) \eta_0^{-r} \eta_1^{-s} = \pm 1$ , а это нам и нужно показать.

Итак, пусть  $\Phi: E(\alpha) \mapsto (r, s)$  — отображение вещественных круговых единиц в  $rs$ -плоскость, неявно определенное равенствами (1). Наша задача — доказать, что образ отображения  $\Phi$  состоит исключительно из точек с целыми координатами. Заметим, что  $\Phi(1) = (0, 0)$ ,  $\Phi(\eta_0) = (1, 0)$ ,  $\Phi(\eta_1) = (0, 1)$ , а также что  $\Phi(E_1 E_2) = \Phi(E_1) + \Phi(E_2)$  при покомпонентном  $((r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2))$  сложении точек на плоскости. Значит, если для некоторой вещественной единицы  $E$  точка

$\Phi(E)$  имеет нецелые координаты, то можно найти такую вещественную единицу  $E_1$ , для которой точка  $\Phi(E_1)$  лежит в квадрате  $\{|r| \leq 1/2, |s| \leq 1/2\}$  и имеет нецелые координаты — для этого нужно лишь положить  $E_1 = E\eta_0^{-\rho}\eta_1^{-\sigma}$ , где  $(\rho, \sigma)$  — ближайшая к  $(r, s)$  точка с целыми координатами, так что  $\rho - 1/2 \leq r \leq \rho + 1/2$ ,  $\sigma - 1/2 \leq s \leq \sigma + 1/2$ . Следовательно, достаточно доказать, что  $\Phi(E)$  может лежать в квадрате  $\{|r| \leq 1/2, |s| \leq 1/2\}$  только в том случае, когда  $\Phi(E) = (0, 0)$ .

Пусть  $E(\alpha)$  — вещественная единица, для которой точка  $\Phi(E) = (r, s)$  лежит в квадрате  $\{|r| \leq 1/2, |s| \leq 1/2\}$ . Тогда

$$\begin{aligned} -\frac{1}{2} \log |\eta_0| - \frac{1}{2} \log |\eta_1| &\leq \log |E(\alpha)| \leq \frac{1}{2} \log |\eta_0| + \frac{1}{2} \log |\eta_1|, \\ -\frac{1}{2} \log |\eta_1| + \frac{1}{2} \log |\eta_2| &\leq \log |E(\alpha^3)| \leq \frac{1}{2} \log |\eta_1| - \frac{1}{2} \log |\eta_2| \end{aligned}$$

(напомним, что число  $\log |\eta_i|$  положительно при  $i = 0, 1$  и отрицательно при  $i = 2$ ). Следовательно,

$$\begin{aligned} |\eta_0\eta_1|^{-1/2} &\leq |E(\alpha)| \leq |\eta_0\eta_1|^{1/2}, \\ |\eta_1/\eta_2|^{-1/2} &\leq |E(\alpha^3)| \leq |\eta_1/\eta_2|^{1/2}. \end{aligned}$$

Можно найти численные значения этих границ:

$$\begin{aligned} 0,667 &\leq |E(\alpha)| \leq 1,499, \\ 0,497 &\leq |E(\alpha^3)| \leq 2,012. \end{aligned}$$

Кроме того, поскольку  $E(\alpha) E(\alpha^3) E(\alpha^2) = \pm \sqrt{NE(\alpha)} = \pm 1$ , получаем

$$0,332 \leq |E(\alpha^2)| \leq 3,017.$$

Остается показать, что никакая вещественная единица, отличная от  $\pm 1$ , не может лежать между этими границами.

Идея остальной части доказательства состоит в том, чтобы написать  $E(\alpha) = a\eta_0 + b\eta_1 + c\eta_2$  и разрешить систему, составленную из этого уравнения и его сопряженных  $E(\alpha^3) = a\eta_1 + b\eta_2 + c\eta_0$ ,  $E(\alpha^2) = a\eta_2 + b\eta_0 + c\eta_1$ , относительно  $a, b, c$  через  $E(\alpha), E(\alpha^3), E(\alpha^2)$ . Это можно сделать, используя соотношения

$$2 + \eta_0^2 + \eta_1^2 + \eta_2^2 = 7, \quad 2 + \eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_0 = 0$$

из § 4.9. В результате найдем

$$\begin{aligned} \eta_0 E(\alpha) + \eta_1 E(\alpha^3) + \eta_2 E(\alpha^2) &= 7a - 2(a + b + c), \\ \eta_1 E(\alpha) + \eta_2 E(\alpha^3) + \eta_0 E(\alpha^2) &= 7b - 2(a + b + c), \\ \eta_2 E(\alpha) + \eta_0 E(\alpha^3) + \eta_1 E(\alpha^2) &= 7c - 2(a + b + c). \end{aligned}$$

Так как  $E(\alpha) + E(\alpha^3) + E(\alpha^2) = -a - b - c$ , то отсюда следует, что

$$7a = (\eta_0 - 2) E(\alpha) + (\eta_1 - 2) E(\alpha^3) + (\eta_2 - 2) E(\alpha^2),$$

$$7b = (\eta_1 - 2) E(\alpha) + (\eta_2 - 2) E(\alpha^3) + (\eta_0 - 2) E(\alpha^2),$$

$$7c = (\eta_2 - 2) E(\alpha) + (\eta_0 - 2) E(\alpha^3) + (\eta_1 - 2) E(\alpha^2).$$

Вещественные числа  $\eta_0, \eta_1, \eta_2$  нам все известны, а границы для  $|E(\alpha)|, |E(\alpha^3)|, |E(\alpha^2)|$  были найдены раньше. Эти соображения сужают границы возможных значений  $a, b, c$ . Так как числа  $a, b, c$  целые, это ограничивает выбор единиц  $E(\alpha)$  — остается *конечное число* возможностей, каждую из которых можно проверить и убедиться, что  $\Phi(E(\alpha))$  не является единицей, лежащей в квадрате  $\{|r| \leq 1/2, |s| \leq 1/2\}$ , за исключением случая, когда  $E(\alpha) = \pm 1$ .

Подробнее, сочетание полученных нами границ для  $|E(\alpha^j)|$  и числовых значений  $\eta_j - 2$  позволяет установить, что числа  $7a, 7b$  и  $7c$  все благополучно меньше 21 по абсолютной величине. Следовательно,  $a, b$  и  $c$  могут иметь лишь значения  $0, \pm 1, \pm 2$ , и вопрос в том, имеется ли среди соответствующих 125 круговых целых единица требуемого вида. Так как  $E(\alpha)$  тогда и только тогда является единицей требуемого вида, когда таковой является и  $-E(\alpha)$ , то можно считать, что  $a \geq 0$ . Так как  $(a + b + c)^3 - 7(a^2b + b^2c + c^2a + abc) = \pm 1$ , то многие из 75 оставшихся возможностей исключаются. (i) Если  $a = 0$ , то имеется 25 возможностей, из которых 9 (при  $b$  или  $c$  равном 0) можно сразу исключить. Случай  $b = -c$  также можно исключить, после чего остается 12 случаев. Можно считать, что  $b$  положительно, поэтому остается только 6 случаев. Из этих круговых целых только 2 являются единицами, а именно  $2\eta_1 + \eta_2$  и  $\eta_1 + \eta_2$ . Поскольку  $\eta_1 + \eta_2 = \eta_0\eta_1$ , точка  $\Phi(\eta_1 + \eta_2) = (1, 1)$  не лежит в квадрате  $\{|r| \leq 1/2, |s| \leq 1/2\}$ . Аналогично,  $2\eta_1 + \eta_2 = -\eta_0\eta_1^2$  (метод проб и ошибок) и  $\Phi(2\eta_1 + \eta_2)$  не лежит в этом квадрате. (ii) Если  $a = 1$ , то имеется 25 возможностей. Те из них, в которых  $b$  или  $c$  равны нулю, охватывались случаем (i). Из 16 оставшихся 10 не дают единиц, а 6 единиц таковы:  $\eta_0 - \eta_1 - \eta_2, \eta_0 - \eta_1 + \eta_2, \eta_0 + \eta_1 - \eta_2, \eta_0 + \eta_1 + \eta_2, \eta_0 + \eta_1 + 2\eta_2, \eta_0 + 2\eta_1 + \eta_2$ . Первые три единицы являются видоизменениями одной:  $\eta_0 - \eta_1 - \eta_2 = 1 + 2\eta_0$ . Вычисляя значение  $\Phi$  от этой единицы, можно найти ее представление в виде  $\pm\eta_0^r\eta_1^s$  и установить, что она не обладает требуемым свойством (упр. 4). Четвертая есть  $\eta_0 + \eta_1 + \eta_2 = -1$ , а пятая и шестая, по существу, не отличаются от  $-1 + \eta_2 = \eta_1^2\eta_2$  (метод проб и ошибок). Таким образом, среди этих единиц ни одна не обладает требуемым свойством. (iii) Если  $a = 2$ , то элементы  $a\eta_0 + b\eta_1 + c\eta_2$ , по существу, совпадают с теми, которые уже проверены в случаях (i) и (ii), кроме тех, для ко-



торых  $b = \pm 2$  и  $c = \pm 2$ . Но в этом случае элемент  $a\eta_0 + b\eta_1 + c\eta_2$  делится на 2 и, следовательно, не является единицей. Это завершает доказательство того, что функция  $\Phi(E(\alpha))$  всегда принимает целые значения, или, что то же самое, что каждая вещественная единица имеет вид  $\pm\eta_0^r\eta_1^s$ .

Сумму  $\sum N(A)^{-s}$  по всем главным дивизорам  $A$  можно теперь рассматривать как сумму по круговым целым. В самом деле, функцию  $\Phi$  можно определить для всех ненулевых круговых целых  $g(\alpha)$  точно так же, как для вещественных единиц  $E(\alpha)$ . Мы просто по определению полагаем, что  $\Phi(g(\alpha)) = (r, s)$  означает следующее:

$$\begin{aligned} r \log |\eta_0| + s \log |\eta_1| &= \log |g(\alpha)|, \\ r \log |\eta_1| + s \log |\eta_2| &= \log |g(\alpha^3)|, \end{aligned}$$

где  $\eta_0, \eta_1, \eta_2, g(\alpha), g(\alpha^3)$  — комплексные числа, которые получаются<sup>1)</sup>, если положить  $\alpha = e^{2\pi i/7}$ . Тогда  $\Phi(e(\alpha)g(\alpha)) = \Phi(e(\alpha)) + \Phi(g(\alpha))$  и, когда  $e(\alpha)$  пробегает все единицы, слагаемое  $\Phi(e(\alpha))$  пробегает все точки  $rs$ -плоскости с целыми координатами. Пусть  $g(\alpha)$  задано, и пусть  $e(\alpha)$  выбрано таким образом, чтобы точка  $\Phi(e(\alpha)) = (\rho, \sigma)$  была близка к точке  $\Phi(g(\alpha)) = (R, S)$  конкретно, пусть  $\rho, \sigma$  выбраны так, что  $\rho \leq R < \rho + 1, \sigma \leq S < \sigma + 1$ . Тогда  $\Phi$ -образ элемента  $e(\alpha)^{-1}g(\alpha)$  лежит в квадрате  $\{0 \leq r < 1, 0 \leq s < 1\}$ . Пусть  $\mathcal{S}$  обозначает этот квадрат. Тогда каждый главный дивизор есть дивизор некоторого  $g(\alpha)$ , для которого точка  $\Phi(g(\alpha))$  лежит в  $\mathcal{S}$ . Если  $g_1(\alpha), g_2(\alpha)$  имеют один и тот же дивизор и если точки  $\Phi(g_1(\alpha)), \Phi(g_2(\alpha))$  обе лежат в  $\mathcal{S}$ , то  $g_1(\alpha) = e(\alpha)g_2(\alpha) = \alpha^k E(\alpha)g_2(\alpha)$ , где  $e(\alpha)$  — единица, а  $E(\alpha)$  — вещественная единица, и точка  $\Phi(g_1(\alpha)) = \Phi(g_2(\alpha)) + \Phi(\alpha^k) + \Phi(E(\alpha)) = \Phi(E(\alpha))$  лежит в квадрате  $\{|r| < 1, |s| < 1\}$ . Это приводит к тому, что  $\Phi(E(\alpha)) = (0, 0)$ ,  $E(\alpha) = \pm 1$ , поэтому отсюда следует, что имеется точно 14 возможных значений  $g_2(\alpha)$ , а именно,  $g_2(\alpha) = \pm g_1(\alpha), \pm \alpha g_1(\alpha), \dots, \pm \alpha^6 g_1(\alpha)$ . Значит, равенство

$$\sum_{A \text{ главный}} N(A)^{-s} = \frac{1}{14} \sum_{\Phi(g(\alpha)) \in \mathcal{S}} N g(\alpha)^{-s}$$

и дает требуемое представление суммы  $\sum N(A)^{-s}$  в виде суммы по круговым целым.

В следующем случае  $\lambda = 11$  можно применить аналогичную процедуру, но проведение вычислений в явном виде становится очень длинным. Однако для осуществления замыслов Куммера — когда нужно проверить условия (A) и (B), но не обязательно вы-

<sup>1)</sup> Если  $g(\alpha) \neq 0$ , то целое число  $N g(\alpha)$  отлично от нуля, а поэтому комплексное число  $g(\alpha)$  отлично от нуля и  $\log |g(\alpha)|$  определен.

числать само число классов — выполнять эти вычисления не требуется, и они могут оставаться неявными.

Начиная изучение случая  $\lambda = 11$ , сначала заметим, что по тем же причинам, что и выше, элемент  $\eta_0 = \alpha + \alpha^{-1} = \alpha + \alpha^{10}$  есть единица; именно,  $\eta_0 = \alpha(1 + \alpha^9) = \alpha(\alpha^{18} - 1)/(\alpha^9 - 1)$ , а это есть единица, умноженная на частное двух круговых целых  $\alpha^7 - 1$  и  $\alpha^9 - 1$  с одним и тем же дивизором  $(\alpha - 1)$ . Следовательно, сопряженные элемента  $\eta_0$  также являются единицами. При примитивном корне  $\gamma = 2$  эти сопряженные обозначаются  $\eta_1 = \alpha^2 + \alpha^{-2}$ ,  $\eta_2 = \alpha^4 + \alpha^{-4}$ ,  $\eta_3 = \alpha^8 + \alpha^{-8}$ ,  $\eta_4 = \alpha^5 + \alpha^{-5}$ . Поскольку  $\eta_0\eta_1\eta_2\eta_3\eta_4 = \pm \sqrt{N\eta_0} = \pm 1$ , каждая вещественная единица вида  $\pm \eta_0^a \eta_1^b \eta_2^c \eta_3^d \eta_4^e$  может быть записана в виде  $\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ . По аналогии с предыдущим случаем естественно спросить, каждая ли вещественная единица  $E(\alpha)$  есть с точностью до знака единица этого вида. Если это так, то для  $r, s, t, u$  выполняются равенства

$$\begin{aligned} r \log|\eta_0| + s \log|\eta_1| + t \log|\eta_2| + u \log|\eta_3| &= \log|E(\alpha)|, \\ r \log|\eta_1| + s \log|\eta_2| + t \log|\eta_3| + u \log|\eta_4| &= \log|E(\alpha^2)|, \\ r \log|\eta_2| + s \log|\eta_3| + t \log|\eta_4| + u \log|\eta_0| &= \log|E(\alpha^4)|, \\ r \log|\eta_3| + s \log|\eta_4| + t \log|\eta_0| + u \log|\eta_1| &= \log|E(\alpha^8)|. \end{aligned} \quad (2)$$

Аналог функции  $\Phi$  ставит в соответствие каждой вещественной единице  $E(\alpha)$  четверку вещественных чисел  $(r, s, t, u)$ , получаемую решением этой системы 4 уравнений с 4 неизвестными. При этом нужно еще доказать, что матрица коэффициентов невырождена.

Анализ этой  $4 \times 4$ -системы упрощается ее симметризацией. Это можно сделать, добавив пятое уравнение  $r \log|\eta_4| + \dots = \log|E(\alpha^{16})|$ , которое вытекает из системы, и добавив в каждое уравнение пятое неизвестное  $v$  с пропущенным коэффициентом, т. е. добавив в первое уравнение слагаемое  $v \log|\eta_4|$ , во второе  $v \log|\eta_0|$  и т. д. Тогда уравнения примут вид

$$M \begin{pmatrix} r \\ s \\ t \\ u \\ v \end{pmatrix} = \begin{pmatrix} \log|E(\alpha)| \\ \log|E(\alpha^2)| \\ \log|E(\alpha^4)| \\ \log|E(\alpha^8)| \\ \log|E(\alpha^{16})| \end{pmatrix}, \quad (3)$$

где  $M$  есть  $5 \times 5$ -матрица

$$M = \begin{pmatrix} \log|\eta_0| & \log|\eta_1| & \log|\eta_2| & \log|\eta_3| & \log|\eta_4| \\ \log|\eta_1| & \log|\eta_2| & \log|\eta_3| & \log|\eta_4| & \log|\eta_0| \\ \log|\eta_2| & \log|\eta_3| & \log|\eta_4| & \log|\eta_0| & \log|\eta_1| \\ \log|\eta_3| & \log|\eta_4| & \log|\eta_0| & \log|\eta_1| & \log|\eta_2| \\ \log|\eta_4| & \log|\eta_0| & \log|\eta_1| & \log|\eta_2| & \log|\eta_3| \end{pmatrix}.$$

Эту матрицу можно было бы назвать *антициклической*, поскольку в ней элемент на  $(i, j)$ -м месте зависит лишь от  $i + j$  по модулю 5. (Говорят, что  $n \times n$ -матрица *циклическая*, если  $a_{ij}$  зависит от  $i - j$  по модулю  $n$ . Другой способ выразить то же самое (см. упр. 5) — это сказать, что линейное отображение  $(x_1, x_2, \dots, x_n) \rightarrow (x_1, x_2, \dots, x_n)$  циклическое, если оно есть полином от отображения «сдвига», которое переводит  $(x_1, x_2, \dots, x_n)$  в  $(x_2, x_3, \dots, \dots, x_n, x_1)$ .) На самом деле перестановка столбцов (перестановка 1-го и 5-го и перестановка 2-го и 4-го) превращает  $M$  в циклическую матрицу. Преимущество от этой замеченной нами особенности заключается в том, что к изучению циклических матриц возможно следующее применение техники анализа Фурье.

*Конечномерный анализ Фурье* сводится, по существу, к следующему: если  $\rho$  — примитивный корень  $n$ -й степени из единицы, то  $n$  векторов  $(1, \rho^j, \rho^{2j}, \dots, \rho^{(n-1)j})$  при  $j = 0, 1, \dots, n-1$  образуют базис, относительно которого все циклические матрицы диагональны. Это замечание (после того как оно сформулировано) совершенно очевидно и может быть доказано различными способами (упр. 6 и 7). (В бесконечномерном анализе Фурье — для рядов Фурье и интегралов Фурье — трудности всегда заключаются в доказательстве *сходимости*, а не в доказательстве алгебраических свойств.) Для циклической матрицы, получающейся из  $M$  перестановкой столбцов, — обозначим ее через  $\tilde{M}$  — диагональная форма по отношению к новому базису имеет на диагонали комплексные числа  $c_j$ , для которых  $\tilde{M} (1, \rho^j, \rho^{2j}, \rho^{3j}, \rho^{4j}) = c_j (1, \rho^j, \rho^{2j}, \rho^{3j}, \rho^{4j})$ , где  $\rho$  — примитивный корень 5-й степени из единицы. Следовательно,  $c_j$  — первая компонента в строке  $\tilde{M} (1, \rho^j, \rho^{2j}, \rho^{3j}, \rho^{4j})$ , представляющая собой выражение

$$c_j = \log |\eta_4| + \rho^j \log |\eta_0| + \rho^{2j} \log |\eta_1| + \rho^{3j} \log |\eta_2| + \rho^{4j} \log |\eta_3|.$$

В частности,  $c_0 = \log |\eta_0 \eta_1 \eta_2 \eta_3 \eta_4| = \log 1 = 0$  и  $\det M = 0$ . Таким образом,  $\det M = 0$ , и система уравнений (3) не может быть решена обращением матрицы  $M$ . Однако остальные значения  $c_j$ , как будет далее показано, все отличны от нуля. Отсюда вытекает, что два вектора могут переходить в один и тот же вектор под действием матрицы  $\tilde{M}$  только в том случае, когда их разность кратна вектору  $(1, 1, 1, 1, 1)$ . Но тогда то же самое верно и для двух векторов, имеющих одинаковый образ при действии матрицы  $M$ . Следовательно, два вектора вида  $(r, s, t, u, 0)$  лишь тогда могут иметь один и тот же образ при действии матрицы  $M$ , когда они совпадают. Но из 4 уравнений системы (2) вытекает 5-е уравнение системы (3), поэтому решение системы (2), если оно существует, единственно. Это показывает, что  $4 \times 4$ -система уравнений (2) является невырожденной и что для любых 4 значений правых частей существуют единственные вещественные числа  $r, s, t, u$ , удо-

влетворяющие системе (2). Следовательно, отображение  $\Phi$  определено корректно.

Остается показать, что числа  $c_1, c_2, c_3, c_4$  отличны от нуля. В действительности Куммер обнаружил, что эти числа, по существу, имеют вид  $L(1, \chi)$ , так что их нетривиальность оказалась следствием теоремы Дирихле о том, что  $L(1, \chi) \neq 0$ . Чтобы найти связь между  $c_j$  и  $L(1, \chi)$ , заметим, во-первых, что  $\eta_0 = \alpha^{-1}(\alpha^2 + 1) = \alpha^{-1}(\alpha^4 - 1)(\alpha^2 - 1)^{-1}$ ,  $\log |\eta_0| = \log |\alpha^4 - 1| - \log |\alpha^2 - 1| = \log |1 - \sigma^2 \alpha| - \log |1 - \sigma \alpha|$ . Значит,  $\log |\eta_k| = \log |1 - \sigma^{2+k} \alpha| - \log |1 - \sigma^{1+k} \alpha|$ . Подстановка этого выражения для  $\log |\eta_k|$  в формулу для  $c_j$  дает

$$c_j = \log |1 - \sigma^6 \alpha| - \log |1 - \sigma^5 \alpha| + \rho^j \log |1 - \sigma^2 \alpha| - \rho^j \log |1 - \sigma \alpha| + \\ + \rho^{2j} \log |1 - \sigma^3 \alpha| - \dots$$

Далее, число  $\sigma^5 \alpha = \alpha^{-1}$  комплексно сопряжено с  $\alpha$ . Значит,  $\log |1 - \sigma^5 \alpha| = \log |1 - \alpha|$ ,  $\log |1 - \sigma^6 \alpha| = \log |1 - \sigma \alpha|$  и т. д. Это дает

$$c_j = \log |1 - \sigma \alpha| + \rho^j \log |1 - \sigma^2 \alpha| + \dots + \rho^{4j} \log |1 - \sigma^5 \alpha| - \\ - \log |1 - \alpha| - \rho^j \log |1 - \sigma \alpha| - \dots - \rho^{4j} \log |1 - \sigma^4 \alpha| = \\ = (\rho^{-j} - 1) [\log |1 - \alpha| + \rho^j \log |1 - \sigma \alpha| + \dots + \rho^{4j} \log |1 - \sigma^4 \alpha|].$$

Конечно, сомножитель  $\rho^{-j} - 1$  отличен от нуля. Если  $\rho = \beta^2$ , где  $\beta$  — примитивный корень 10-й степени из единицы, то второй сомножитель в выражении для  $c_j$  в точности равен числу, которое в § 6.6 было обозначено через  $C_j$ . Так как числа  $L(1, \chi_{2j})$  кратны числам  $C_j$  и  $L(1, \chi_{2j}) \neq 0$ , то это и доказывает, что  $c_j \neq 0$ .

Этим завершается доказательство того, что система (2) действительно определяет в неявной форме функцию из множества вещественных круговых единиц  $E(\alpha)$  в множество четверок  $(r, s, t, u)$  вещественных чисел. Ясно, что  $\Phi(1) = (0, 0, 0, 0)$ ,  $\Phi(\eta_0) = (1, 0, 0, 0)$ ,  $\Phi(\eta_1) = (0, 1, 0, 0)$ ,  $\Phi(\eta_2) = (0, 0, 1, 0)$ ,  $\Phi(\eta_3) = (0, 0, 0, 1)$ ,  $\Phi(\eta_4) = (-1, -1, -1, -1)$  и  $\Phi(E_1 E_2) = \Phi(E_1) + \Phi(E_2)$ . Отсюда следует, что каждая четверка *целых* чисел  $(r, s, t, u)$  есть  $\Phi$ -образ некоторой вещественной единицы  $E$ , а на самом деле эта четверка является  $\Phi$ -образом точно двух вещественных единиц  $\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ , поскольку из  $\Phi(E) = (0, 0, 0, 0)$  вытекает, что  $\log |E(\alpha)| = 0$ , откуда  $E(\alpha) = \pm 1$ , ибо  $E(\alpha)$  вещественна. Вопрос о том, существуют ли вещественные единицы, отличные от тех, которые имеют вид  $\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ , равносильно, следовательно, вопросу о том, может ли функция  $\Phi(E(\alpha))$  принимать нецелые значения.

Как и в предыдущем случае, при поиске вещественных единиц  $E(\alpha) = a\eta_0 + b\eta_1 + c\eta_2 + d\eta_3 + e\eta_4$ , не имеющих вида

$\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ , можно ограничиться теми единицами  $E(\alpha)$ , для которых точка  $\Phi(E(\alpha))$  лежит в области  $\{|r| \leq 1/2, |s| \leq 1/2, |t| \leq 1/2, |u| \leq 1/2\}$ . Как и раньше, предположение о том, что  $\Phi(E(\alpha))$  лежит в этой области, устанавливает границы для  $\log |E(\alpha^j)|$  и, следовательно, для  $E(\alpha^j)$  при  $j = 1, 2, \dots, 5$ . Затем из этих границ в сочетании с равенствами

$$11a = (\eta_0 - 2)E(\alpha) + (\eta_1 - 2)E(\alpha^2) + (\eta_2 - 2)E(\alpha^4) + \\ + (\eta_3 - 2)E(\alpha^3) + (\eta_4 - 2)E(\alpha^5),$$

$$11b = \text{и т.д.}$$

(которые выводятся точно так же, как и в случае  $\lambda = 7$ ) получаются границы для  $a, b, c, d, e$ . Но эти числа — *целые*, поэтому для  $E$  остается лишь конечное число возможностей. Для каждого из отобранных круговых целых мы можем вычислить норму и исключить из рассмотрения те элементы, которые не являются единицами. Пусть  $E_1, E_2, \dots, E_N$  — вещественные единицы, которые в результате остались. Мы можем вычислить  $\Phi(E_1), \Phi(E_2), \dots, \Phi(E_N)$  и исключить те  $E_i$ , для которых  $\Phi(E_i)$  не лежит в области  $\{|r| \leq 1/2, |s| \leq 1/2, |t| \leq 1/2, |u| \leq 1/2\}$ .

Если это проделать, то, как и в случае  $\lambda = 7$ , обнаружится, что все  $E_i$  исключены, и, таким образом, отсюда следует, что все вещественные единицы имеют вид  $\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ . Однако доказательство Куммера Последней теоремы Ферма для  $\lambda = 11$  не использует этого факта; не нужно выполнять описанные выше очень длинные вычисления в явном виде, а взамен можно провести рассуждение неявного типа следующим образом.

Если мы наталкиваемся в списке на единицу  $E_i$ , которая не имеет вида  $\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ , то мы можем так перенумеровать единицы списка, что она будет обозначена через  $E_1$ . Затем для каждой из остальных единиц мы сможем проверить, имеет ли она вид  $\pm \eta_0^r \eta_1^s \eta_2^t \eta_3^u$  или вид  $\pm E_1 \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ . Если это так, то такая единица исключается из списка. Если же нет, то обозначим ее через  $E_2$  и продолжим процесс. Этот процесс завершается списком  $E_1, E_2, \dots, E_n$  вещественных единиц, обладающих таким свойством: *каждая вещественная единица  $E$  может быть записана точно одним способом в виде  $E = \pm E_i \eta_0^r \eta_1^s \eta_2^t \eta_3^u$  при некотором выборе знака, при некоторых целых числах  $r, s, t, u$  и при некотором выборе  $i = 0, 1, 2, \dots, n$ , считая, по определению,  $E_0 = 1$ . Чтобы в этом убедиться, достаточно заметить, что  $r, s, t, u$  можно выбрать таким способом, что значение функции  $\Phi$  от  $E \eta_0^{-r} \eta_1^{-s} \eta_2^{-t} \eta_3^{-u}$  лежит в области  $\{|r| \leq 1/2, |s| \leq 1/2, |t| \leq 1/2, |u| \leq 1/2\}$  и, следовательно, эта единица содержится в первоначальном списке  $E_1, E_2, \dots, E_N$ ; значит, в силу самого способа получения окончательного списка из первоначального исключением элементов,*

единица  $E\eta_0^{-r}\eta_1^{-s}\eta_2^{-t}\eta_3^{-u}$  есть либо  $\pm 1$ , либо  $\pm E_i\eta_0^r\eta_1^s\eta_2^t\eta_3^u$  точно для одной из единиц  $E_i$  окончательного списка.

По причинам, которые выяснятся в § 6.14, число  $n + 1$  вещественных единиц окончательного списка, дополненного единицей  $E_0 = 1$ , называется *вторым сомножителем числа классов* и обозначается через  $h_2$ . Как было выше отмечено,  $h_2 = 1$  в случае  $\lambda = 11$ , но нам это не понадобится.

Теперь сумму чисел  $N(A)^{-s}$  по всем главным дивизорам можно записать в виде суммы по круговым целым, продолжив вначале функцию  $\Phi$  на все круговые целые, как это было сделано выше в случае  $\lambda = 7$ . Неявное определение функции  $\Phi$  равенствами (2) в том виде, как оно есть, точно так же применимо к произвольному круговому целому  $g(\alpha)$ , как и к вещественным круговым единицам  $E(\alpha)$ . Таким способом  $\Phi$  определена как функция, отображающая круговые целые в четверки вещественных чисел, причем  $\Phi(g_1(\alpha)g_2(\alpha)) = \Phi(g_1(\alpha)) + \Phi(g_2(\alpha))$ . Если теперь  $A$  — данный главный дивизор, например дивизор кругового целого  $g(\alpha)$ , то каждое круговое целое, дивизор которого есть  $A$ , может быть записано точно одним способом в виде  $\pm \alpha^k E_i(\alpha) \eta_0^r \eta_1^s \eta_2^t \eta_3^u g(\alpha)$ . Следовательно,  $\Phi$ -образ круговых целых с дивизором  $A$  состоит в точности из четверок вида  $\Phi(E_i(\alpha)) + \Phi(g(\alpha)) + (r, s, t, u)$  и на каждую из этих точек отображаются точно  $22$  круговых целых. Если задана любая из  $h_2$  единиц  $E_i(\alpha)$ , то, очевидно, можно найти одну и только одну такую четверку  $(r, s, t, u)$ , что эта точка лежит в области  $\mathcal{S} = \{(r, s, t, u): 0 \leq r < 1, 0 \leq s < 1, 0 \leq t < 1, 0 \leq u < 1\}$ . Следовательно, точно  $22h_2$  круговых целых  $g(\alpha)$  с дивизором  $A$  обладают тем свойством, что  $\Phi(g(\alpha))$  лежит в  $\mathcal{S}$ , и поэтому

$$\sum_{A \text{ главный}} N(A)^{-s} = \frac{1}{22h_2} \sum_{\Phi(g(\alpha)) \in \mathcal{S}} N(g(\alpha))^{-s}.$$

Это и есть запись искомой суммы в виде суммы по круговым целым.

В общем случае требуемая процедура является прямым обобщением того, что мы видели в случае  $\lambda = 11$ , за исключением одного момента, а именно, выбора базисных единиц  $\eta_0, \eta_1, \eta_2, \dots$ . Хотя и верно то, что периоды длины 2 всегда являются единицами, однако легко указать формулу для единиц, которая, вообще говоря, включает больше единиц, чем формула  $\pm \eta_0^r \eta_1^s \eta_2^t \dots$ , использованная выше. Эта формула имеет вид

$$\pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}, \quad (4)$$

где  $\mu = (\lambda - 1)/2$ , а целые числа  $x_1, x_2, \dots, x_\mu$  таковы, что  $x_1 + x_2 + \dots + x_\mu = 0$ . Такое выражение является *единицей*, поскольку каждый член произведения имеет вид единица  $\cdot (1 - \alpha)^{x_j}$ , а произведение сомножителей  $(1 - \alpha)^{x_j}$  исчезает. В случае  $\lambda = 11$



эта формула дает не больше единиц, чем формула  $\pm \alpha^k \eta_0^r \eta_1^s \eta_2^t \eta_3^u$ , поскольку  $\eta_0 = \alpha + \alpha^{-1} = \alpha^{-1} (\alpha^2 + 1) = \alpha^{-1} (\alpha^4 - 1) (\alpha^2 - 1)^{-1} = \alpha^{-1} (1 - \sigma^2 \alpha) (1 - \sigma \alpha)^{-1}$ , и всегда возможно решить относительно  $k, r, s, t, u$  следующее уравнение:

$$\begin{aligned} (1 - \sigma \alpha)^{x_1} (1 - \sigma^2 \alpha)^{x_2} \dots (1 - \sigma^5 \alpha)^{x_5} &= \pm \alpha^k \eta_0^r \eta_1^s \eta_2^t \eta_3^u = \\ &= \pm \alpha^{k-r-2s-4t-8u} (1 - \sigma^2 \alpha)^r (1 - \sigma \alpha)^{-r} (1 - \sigma^3 \alpha)^s (1 - \sigma^2 \alpha)^{-s} \dots (1 - \\ &\quad - \sigma^4 \alpha)^{-u} = \\ &= \pm \alpha^{k-r-2s-4t-8u} (1 - \sigma \alpha)^{-r} (1 - \sigma^2 \alpha)^{r-s} (1 - \sigma^3 \alpha)^{s-t} (1 - \sigma^4 \alpha)^{t-u} (1 - \\ &\quad - \sigma^5 \alpha)^u, \end{aligned}$$

где данные числа  $x_1, x_2, x_3, x_4, x_5$  удовлетворяют равенству  $x_1 + x_2 + x_3 + x_4 + x_5 = 0$ . (Действительно,  $k \equiv r + 2s + 4t + 8u \pmod{11}$ ,  $r = -x_1$ ,  $s = -x_1 - x_2$ ,  $t = -x_1 - x_2 - x_3$ ,  $u = -x_1 - x_2 - x_3 - x_4 = x_5$ .) Однако в случае  $\lambda = 17$  имеются единицы вида (4), непредставимые в виде  $\eta_0^r \eta_1^s \eta_2^t \eta_3^u \eta_4^v \eta_5^w \eta_6^x \eta_7^y$  (см. упр. 8). Значит, в общем случае лучше попытаться записывать единицы в виде (4), чем рассматривать их как произведения периодов длины 2 на  $\pm \alpha^k$ . Это и будет сделано в следующем параграфе.

## Упражнения

1. Докажите, что при  $\lambda = 5$  вещественные единицы  $\pm \theta^j$  ( $\theta = \alpha + \alpha^4$ ,  $j$  — целое число) различны [легкая часть утверждения] и охватывают все вещественные единицы. [Решите уравнение Пелля или воспользуйтесь способом, предлагаемым в тексте.]

2. Пусть  $\lambda = 7$  и  $\eta_0, \eta_1, \eta_2$  — периоды длины 2. Вычислите произведение трех сопряженных элемента  $a\eta_0 + b\eta_1 + c\eta_2$  ( $a, b, c$  — целые числа).

3. Докажите, что если  $E(\alpha) = a\eta_0 + b\eta_1 + \dots + c\eta_{\mu-1}$ , то  $\lambda a = (\eta_0 - 2) E(\alpha) + (\eta_1 - 2) \sigma E(\alpha) + \dots + (\eta_{\mu-1} - 2) \sigma^{\mu-1} E(\alpha)$ .

4. При  $\lambda = 7$  запишите  $1 + 2\eta_0$  в виде  $\pm \eta_0^r \eta_1^s$ . [Воспользуйтесь либо методом проб и ошибок, либо предложенным в тексте способом вычисления значения  $\Phi(1 + 2\eta_0)$ .]

5. Покажите, что линейное преобразование вида  $y_i = \sum_{j=1}^n a_{ij} x_j$ , матрица коэффициентов которого *циклическая* (т. е.  $a_{i+1, j+1} = a_{i, j}$  для всех  $i, j$ , рассматриваемых как вычеты по модулю  $n$ ), может быть записано как полином от линейного преобразования  $y_1 = x_2, y_2 = x_3, \dots, y_{n-1} = x_n, y_n = x_1$ . Здесь линейные преобразования понимаются как отображения множества  $\mathbb{R}^n$  наборов из  $n$  вещественных переменных в себя, поэтому имеют смысл *произведение* (суперпозиция) и *сумма* (поточечное сложение) линейных преобразований.

6. Докажите, что если  $\rho$  — примитивный корень  $n$ -й степени из единицы, то  $n$  векторов  $(1, \rho^j, \rho^{2j}, \dots, \rho^{(n-1)j})$  при  $j = 0, 1, \dots, n-1$  линейно независимы. Это можно сформулировать по-другому: покажите, что система уравнений

$$y_i = \sum_{j=0}^{n-1} \rho^{ij} x_j \text{ имеет единственное решение } (x_0, x_1, \dots, x_{n-1}) \text{ для каждого}$$

заданного набора  $(y_0, y_1, \dots, y_{n-1})$ . Самый простой способ доказательства заключается в построении *явного решения*, как это было сделано для частного случая  $\lambda = 5$  в § 6.5. Это даст *формулу обратного преобразования Фурье* в этом конечномерном случае. По существу, это есть не что иное, как утверждение об ортогональности векторов  $(1, \rho^j, \dots, \rho^{-j})$ .

7. Покажите, что если  $M$  — циклическая матрица, то применение ее к векторам  $(1, \rho^j, \rho^{2j}, \dots, \rho^{-j})$  переводит ее в кратную ей матрицу. [Благодаря упр. 5 достаточно доказать это для преобразования сдвига  $y_i = x_{i+1}, y_n = x_1$ , а это тривиально.] Выведите отсюда, что в базисе  $(1, \rho^j, \rho^{2j}, \dots, \rho^{-j})$  матрица  $M$  становится диагональной. Это означает, что если  $y_i = \sum \rho^{ij} x_j$ , то применение матрицы  $M$  к вектору  $y$  всего лишь умножает каждую координату  $x_j$  вектора  $x$  на некоторую постоянную  $c_j$ .

8. В случае  $\lambda = 17$  найдите единицу вида (4), которая не является произведением периодов длины 2 на  $\pm \alpha^k$ . При каких условиях на  $\lambda$  можно сказать, что все единицы вида (4) являются произведениями периодов длины 2 на  $\pm \alpha^k$ ? Условия должны охватывать случаи  $\lambda < 17$ .

## 6.10. Единицы: общий случай

Пусть, как обычно,  $\lambda$  — простое число, большее двух, и пусть  $\mu = (\lambda - 1)/2$ . Тогда для любых целых чисел  $x_1, x_2, \dots, x_\mu$ , удовлетворяющих условию  $x_1 + x_2 + \dots + x_\mu = 0$ , круговое целое

$$\pm \alpha^k (1 - \sigma \alpha)^{x_1} (1 - \sigma^2 \alpha)^{x_2} \dots (1 - \sigma^\mu \alpha)^{x_\mu} \quad (1)$$

(здесь через  $\sigma$  обозначается сопряжение, переводящее  $\alpha$  в  $\alpha^\gamma$ , где  $\gamma$  — примитивный корень по модулю  $\lambda$ ) корректно определено (несмотря на наличие отрицательных показателей) и является единицей. Это следует из того, что  $(1 - \sigma^j \alpha) / (1 - \alpha)$  есть единица для каждого  $j$ , а тогда, как легко заметить, (1) является произведением единиц на  $(1 - \alpha)^{x_1 + x_2 + \dots + x_\mu} = (1 - \alpha)^0 = 1$ .

Для данного кругового целого  $g(\alpha)$  обозначим через  $Lg(\alpha)$  вектор, имеющий следующие  $\mu$  компонент:  $\log |g(\alpha)|$ ,  $\log |\sigma g(\alpha)|$ ,  $\dots$ ,  $\log |\sigma^{\mu-1} g(\alpha)|$  (через  $|\cdot|$  обозначен модуль комплексного числа при условии  $\alpha = e^{2\pi i/\lambda}$ ). Если данную круговую единицу  $e(\alpha)$  можно записать в виде (1), то, очевидно,

$$Le(\alpha) = x_1 L(1 - \sigma \alpha) + x_2 L(1 - \sigma^2 \alpha) + \dots + x_\mu L(1 - \sigma^\mu \alpha). \quad (2)$$

Этим равенством числа  $x_1, x_2, \dots, x_\mu$  определяются однозначно, что можно доказать следующим образом.

Рассмотрим  $\mu \times \mu$ -матрицу  $M$ , столбцами которой являются векторы  $L(1 - \sigma \alpha)$ ,  $L(1 - \sigma^2 \alpha)$ ,  $\dots$ ,  $L(1 - \sigma^\mu \alpha)$ . Тогда (2) означает, что если умножить  $M$  на вектор-столбец  $(x_1, x_2, \dots, x_\mu)$ , то получится вектор-столбец  $Le(\alpha)$ . Матрица  $M$  *антициклическа* в смысле предыдущего параграфа, т. е. элемент, стоящий в  $i$ -й строке и  $j$ -м столбце, есть  $\log |1 - \sigma^{i+j-1} \alpha|$  и, поскольку  $\sigma^\mu \alpha = \alpha^{-1} = \bar{\alpha}$  и  $\log |\bar{z}| = \log |z|$ , величина этого элемента

зависит только от  $i + j$  по модулю  $\mu$ . Пусть  $\tilde{M}$  — матрица, получаемая из  $M$  путем перестановки столбцов первого с последним, второго с предпоследним и т. д. Тогда матрица  $\tilde{M}$  циклична и диагонализирована базисом  $(1, \rho^j, \rho^{2j}, \dots, \rho^{-j})$ , где  $j = 0, 1, \dots, \mu - 1$ , а  $\rho$  — примитивный корень  $\mu$ -й степени из единицы. Следовательно, определитель матрицы  $\tilde{M}$  есть произведение чисел  $c_j$ , определенных равенством  $\tilde{M} (1, \rho^j, \dots, \rho^{-j}) = c_j (1, \rho^j, \dots, \rho^{-j})$ . Таким образом,

$$c_j = \log |1 - \sigma^\mu \alpha| + \rho^j \log |1 - \sigma \alpha| + \dots + \rho^{(\mu-1)j} \log |1 - \sigma^{\mu-1} \alpha|.$$
 Для  $j = 0$  это дает  $c_0 = \log |1 - \sigma \alpha| + \log |1 - \sigma^2 \alpha| + \dots + \log |1 - \sigma^\mu \alpha| = \frac{1}{2} [\log |1 - \sigma \alpha| + \log |1 - \sigma^2 \alpha| + \dots + \log |1 - \sigma^{\mu-1} \alpha|] = \frac{1}{2} \log N (1 - \alpha) = \log \sqrt{\lambda}$ . Для следующих значений  $j = 1, 2, \dots, \mu - 1$  мы получаем  $c_j = C_j$ , где величина  $C_j$  определяется, как в § 6.6, при  $\rho = \beta^{-2}$ . Следовательно,  $\det \tilde{M} = \log \sqrt{\lambda} \cdot C_1 C_2 \dots C_{\mu-1}$ , и так как ни один из сомножителей здесь не равен нулю (число  $L(1, \chi_{2j}) \neq 0$  кратно  $C_j$ ), то  $\tilde{M}$  — обратимая матрица. Но  $\tilde{M}$  является матрицей коэффициентов системы (2) (после перестройки уравнений этой системы), поэтому отсюда следует, что система (2) разрешима, что и требовалось показать.

Таким образом, система уравнений (2) определяет функцию, отображающую некоторые круговые единицы в наборы  $(x_1, x_2, \dots, x_\mu)$  из  $\mu$  целых чисел. На самом деле это определение может быть расширено на все круговые целые  $g(\alpha)$ . Пусть  $\Phi$  обозначает эту функцию, т. е. пусть  $\Phi(g(\alpha))$  представляет собой такой набор  $(x_1, x_2, \dots, x_\mu)$  из  $\mu$  вещественных чисел, что

$$Lg(\alpha) = x_1 L(1 - \sigma \alpha) + x_2 L(1 - \sigma^2 \alpha) + \dots + x_\mu L(1 - \sigma^\mu \alpha). \quad (3)$$

Тогда функция  $\Phi$  переводит круговую единицу вида (1) в набор  $(x_1, x_2, \dots, x_\mu)$  из  $\mu$  целых чисел, для которых  $x_1 + x_2 + \dots + x_\mu = 0$ . Обобщая это, можно утверждать, что  $g(\alpha)$  тогда и только тогда является единицей, когда  $\Phi(g(\alpha)) = (x_1, x_2, \dots, x_\mu)$  обладает тем свойством, что  $x_1 + x_2 + \dots + x_\mu = 0$ . Это можно доказать следующим образом.

Сумма компонент вектора, стоящего в левой части (3), равна  $\log |g(\alpha)| + \log |\sigma g(\alpha)| + \dots + \log |\sigma^{\mu-1} g(\alpha)|$ . Так как  $\log |\sigma^{\mu+k} g(\alpha)| = \log |\sigma^k g(\alpha)|$ , эта сумма равна  $\frac{1}{2} \log Ng(\alpha)$ . С другой стороны, она равна числу  $x_1$ , умноженному на сумму компонент вектора  $L(1 - \sigma \alpha)$ , плюс число  $x_2$ , умноженное на сумму компонент вектора  $L(1 - \sigma^2 \alpha)$ , и т. д. Поскольку сумма

компонент вектора  $L(1 - \sigma^k \alpha)$  равна  $\frac{1}{2} \log N(1 - \sigma^k \alpha) = \frac{1}{2} \log \lambda$  для всех  $k$ , отсюда и из (3) вытекает, что

$$\frac{1}{2} \log Ng(\alpha) = \frac{1}{2} (\log \lambda) (x_1 + x_2 + \dots + x_\mu),$$

т.е.

$$x_1 + x_2 + \dots + x_\mu = \frac{\log Ng(\alpha)}{\log \lambda} = \log_\lambda Ng(\alpha).$$

Это тождество будет полезно в дальнейшем. В частности, круговое целое  $g(\alpha)$  тогда и только тогда является единицей, когда  $x_1 + x_2 + \dots + x_\mu = 0$ , что и нужно было показать.

Будем называть две единицы *эквивалентными*, если их частное является единицей вида (1). Это же самое можно сказать так:  $e_1(\alpha)$  и  $e_2(\alpha)$  эквивалентны, если  $\Phi(e_1(\alpha)) - \Phi(e_2(\alpha))$  имеет целые компоненты (см. упр. 2). Тогда ясно, что каждая единица  $e(\alpha)$  эквивалентна такой единице,  $\Phi$ -образ которой имеет вид  $(x_1, x_2, \dots, x_\mu)$ , где  $|x_1| \leq 1/2, |x_2| \leq 1/2, \dots, |x_{\mu-1}| \leq 1/2$ . Имеется лишь конечное число единиц, удовлетворяющих этому условию, и все они могут быть найдены следующим образом. Из ограничений  $|x_1| \leq 1/2, |x_2| \leq 1/2, \dots, |x_{\mu-1}| \leq 1/2$  вытекает неравенство  $|x_\mu| \leq (\mu - 1)/2$  (ибо для единицы сумма этих чисел равна 0), а тогда из определения (2) функции  $\Phi$  вытекает, что все  $\mu$  компонент вектора  $Le(\alpha)$  ограничены, и их границы можно получить в явном виде. Значит,  $|e(\alpha^j)|$  ограничены для всех  $j = 1, 2, \dots, \lambda - 1$ . Так как  $e(\alpha) = \alpha^k E(\alpha)$ , где  $E(\alpha)$  — вещественная единица, скажем  $E(\alpha) = a\eta_0 + b\eta_1 + \dots + c\eta_{\mu-1}$ , где  $a, b, \dots, c$  — целые числа, а  $\eta_0, \eta_1, \dots, \eta_{\mu-1}$  — периоды длины 2, то границы для  $|e(\alpha^j)|$  являются границами для  $|E(\alpha^j)|$ , а этими границами можно воспользоваться в соотношениях

$$\begin{aligned} \lambda a &= (\eta_0 - 2) E(\alpha) + (\eta_1 - 2) \sigma E(\alpha) + \dots \\ &\quad \dots + (\eta_{\mu-1} - 2) \sigma^{\mu-1} E(\alpha), \\ \lambda b &= \text{и т. д.} \end{aligned}$$

и получить границы для чисел  $a, b, \dots, c$ . Но эти числа — *целые*, поэтому для них имеется лишь конечное множество возможных значений, а следовательно, для  $E(\alpha)$  и  $e(\alpha) = \alpha^k E(\alpha)$  тоже имеется лишь конечное множество возможностей.

Из этого конечного списка можно исключить все неединицы. Таким способом мы получим конечный список  $E_1(\alpha), E_2(\alpha), \dots, E_N(\alpha)$  вещественных единиц, обладающий тем свойством, что каждая единица эквивалентна одной из  $E_i(\alpha)$ . Не умаляя общности, можно считать, что  $E_1(\alpha) = 1$ , а затем, последовательно исключая повторения, т. е. отбрасывая те  $E_i(\alpha)$ , которым найдется эквивалентная единица среди уже оставленных, мы получаем список, обладающий тем свойством, что каждая единица

эквивалентна одной и только одной единице из списка. Пусть  $h_2$  — число единиц в этом окончательном списке. В другой форме сказать, что каждая единица  $e(\alpha)$  эквивалентна одной и только одной единице из  $E_i$  ( $i = 1, 2, \dots, h_2$ ), можно так: каждая единица допускает одно и только одно представление в виде  $\pm \alpha^k E_i (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$ . Это дает полное описание круговых единиц.

Пусть теперь  $A$  — главный дивизор, и пусть  $g(\alpha)$  — круговое целое, дивизором которого является  $A$ . Для каждой из  $h_2$  построенных нами единиц  $E_i(\alpha)$  существует круговое целое  $g_i(\alpha)$  вида  $g_i(\alpha) = \pm \alpha^k E_i(\alpha) (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu} g(\alpha)$ ,  $\Phi$ -образ которого имеет неотрицательные и меньшие числа 1 первые  $\mu - 1$  компонент. Действительно, сомножитель  $\pm \alpha^k$  произволен ( $2\lambda$  способов выбора), но целые числа  $x_1, x_2, \dots, x_\mu$  однозначно определяются условием, что величина  $x_j$  в сумме с  $j$ -й компонентой разности  $\Phi(E_i(\alpha)) - \Phi(g(\alpha))$  неотрицательна и  $< 1$  для  $j = 1, 2, \dots, \mu - 1$ , а также условием, что  $x_1 + x_2 + \dots + x_\mu = 0$ . Следовательно, имеется точно  $2\lambda$  круговых целых  $g_i(\alpha)$ , удовлетворяющих этим условиям. Но индекс  $i$  может принимать любое одно из  $h_2$  значений, поэтому найдется точно  $2\lambda h_2$  круговых целых вида  $e(\alpha) g(\alpha)$  (т. е. круговых целых, дивизор которых есть  $A$ ),  $\Phi$ -образы которых имеют свои первые  $\mu - 1$  компонент  $\geq 0$  и  $< 1$ . Таким образом, если через  $\mathcal{S}$  обозначена область  $\{(x_1, x_2, \dots, x_\mu): 0 \leq x_1 < 1, 0 \leq x_2 < 1, \dots, 0 \leq x_{\mu-1} < 1, x_\mu \text{ не ограничено}\}$ , то

$$\sum_{A \text{ главный}} N(A)^{-s} = \frac{1}{2\lambda h_2} \sum_{\Phi(g(\alpha)) \in \mathcal{S}} N g(\alpha)^{-s}.$$

Это и есть требуемое представление левой части в виде суммы по круговым целым.

## Упражнения

1. Докажите, что отношение эквивалентности для единиц, приведенное в тексте, рефлексивно, симметрично, транзитивно и согласовано с умножением.

2. Ясно, что если единицы  $e_1(\alpha)$  и  $e_2(\alpha)$  эквивалентны, то разность  $\Phi(e_1(\alpha)) - \Phi(e_2(\alpha))$  имеет целые компоненты. Докажите обратное утверждение.

## 6.11. Вычисление интеграла

В § 6.3 было найдено, как стремится к  $\infty$  при  $s \downarrow 1$  сумма  $\sum n^{-s}$ . Для этого сначала было доказано, что сумма отличается на ограниченную величину от соответствующего интеграла  $\int_1^\infty x^{-s} dx$ , а

затем этот интеграл был вычислен по обычным правилам. Точно так же, имеется интеграл, отличающийся на ограниченную величину от суммы  $\sum Ng(\alpha)^{-s}$  по всем тем  $g(\alpha)$ , для которых  $\Phi(g(\alpha))$  лежит в  $\mathcal{S}$ , т. е. в области, с которой мы встречались в предыдущем параграфе. Это интеграл

$$\int_{\mathcal{D}} N(u_1\sigma\alpha + u_2\sigma^2\alpha + \dots + u_{\lambda-1}\sigma^{\lambda-1}\alpha)^{-s} du_1 du_2 \dots du_{\lambda-1}, \quad (1)$$

где  $u_1, u_2, \dots, u_{\lambda-1}$  — вещественные переменные, функции  $N$  и  $\Phi$ , первоначально определенные для круговых целых  $u_1\sigma\alpha + u_2\sigma^2\alpha + \dots + u_{\lambda-1}\sigma^{\lambda-1}\alpha$  (при целых  $u_j$ ), продолжены очевидным образом на произвольные вещественные значения переменных  $u_j$ , а область интегрирования  $\mathcal{D}$  представляет собой множество всех точек,  $\Phi$ -образы которых лежат в  $\mathcal{S} = \{(x_1, x_2, \dots, x_\mu) : 0 \leq x_1 < 1, 0 \leq x_2 < 1, \dots, 0 \leq x_{\mu-1} < 1, x_\mu \text{ не ограничено}\}$ . Точнее, пусть  $g(\alpha)$  обозначает  $u_1\sigma\alpha + u_2\sigma^2\alpha + \dots + u_{\lambda-1}\sigma^{\lambda-1}\alpha$ , где  $u_j$  не обязательно целые, пусть  $Lg(\alpha)$  — вектор-столбец  $(\log |g(\alpha)|, \log |\sigma g(\alpha)|, \dots, \log |\sigma^{\mu-1}g(\alpha)|)$ , где  $|g(\alpha)|$  — модуль комплексного числа  $g(\alpha)$ , если положить  $\alpha = e^{2\pi i/\lambda}$ , пусть  $Ng(\alpha)$  — вещественное число  $g(\alpha) \cdot \sigma g(\alpha) \cdot \dots \cdot \sigma^{\lambda-1}g(\alpha)$ , и пусть  $\Phi$  — функция, определенная неявно формулой  $\Phi(g(\alpha)) = (x_1, x_2, \dots, x_\mu)$ , где

$$Lg(\alpha) = x_1 L(1 - \sigma\alpha) + x_2 L(1 - \sigma^2\alpha) + \dots + x_\mu L(1 - \sigma^\mu\alpha).$$

Функции  $Ng(\alpha)^{-s}$  и  $Lg(\alpha)$  определены лишь тогда, когда  $g(\alpha)$ , рассматриваемое как комплексное число, отлично от нуля. Это имеет место тогда и только тогда, когда  $Ng(\alpha) \neq 0$ . Значит, с самого начала нужно исключить из области интегрирования  $\mathcal{D}$  те точки, для которых  $Ng(\alpha) = 0$ . Фактически, для того чтобы избавиться от точек, для которых  $Ng(\alpha)^{-s}$  велико, естественно исключить из  $\mathcal{D}$  те точки, для которых  $Ng(\alpha) < 1$ . При этом не будет исключено ни одно круговое целое, кроме  $g(\alpha) = 0$ . Таким образом,  $\mathcal{D}$  будет представлять собой множество всех  $g(\alpha)$  в пространстве переменных  $u_1, u_2, \dots, u_{\lambda-1}$ , для которых  $Ng(\alpha) \geq 1$  и для которых  $\Phi(g(\alpha))$  (которое определено, поскольку  $Ng(\alpha) \neq 0$ ) лежит в  $\mathcal{S}$ .

В следующем параграфе будет показано, что несобственный интеграл (1) сходится при  $s > 1$  и что его значение при  $s \downarrow 1$  отличается на ограниченную величину от  $\sum Ng(\alpha)^{-s}$  (где  $g(\alpha)$  — круговое целое из  $\mathcal{D}$ ). Этот параграф посвящен явному вычислению интеграла при помощи замен переменных и применения основной теоремы интегрального исчисления.



В качестве первого шага этого вычисления произведем комплексную замену переменных:  $z_k = u_1 \sigma^k \alpha + u_2 \sigma^{k+1} \alpha + \dots + u_{\lambda-1} \sigma^{k-1} \alpha$  для  $k = 1, 2, \dots, \lambda - 1$ . Число  $\sigma^{k+\mu} \alpha$  комплексно сопряжено числу  $\sigma^k \alpha$ , поэтому  $z_{k+\mu}$  и  $z_k$  комплексно сопряжены для вещественных значений переменных  $u_i$ . Значит, если вещественные числа  $v_k, w_k$  определены равенствами  $z_k = v_k + iw_k$ , то  $\lambda - 1$  величин  $v_1, v_2, \dots, v_\mu, w_1, w_2, \dots, w_\mu$  являются вещественнозначными функциями от переменных  $u_1, u_2, \dots, u_{\lambda-1}$ , причем  $z_k = v_k + iw_k, z_{\mu+k} = v_k - iw_k$ . В интеграле (1) можно следующим образом перейти к переменным  $v_k, w_k$ . Пусть  $A$  — комплексная  $(\lambda - 1) \times (\lambda - 1)$ -матрица, определяющая преобразование  $z = Au$ . Тогда на основании правил оперирования с дифференциальными формами (см. [E1])  $dz_1 dz_2 \dots dz_{\lambda-1} = \det A du_1 du_2 \dots du_{\lambda-1}$ . С другой стороны,

$$\begin{aligned} dz_1 dz_2 \dots dz_{\lambda-1} &= (dv_1 + idw_1)(dv_2 + idw_2) \dots (dv_\mu + idw_\mu) \times \\ &\quad \times (dv_1 - idw_1)(dv_2 - idw_2) \dots (dv_\mu - idw_\mu) = \\ &= \pm \prod_{k=1}^{\mu} (dv_k + i dw_k)(dv_k - i dw_k) = \pm \prod_{k=1}^{\mu} (-2i dv_k dw_k) = \\ &= \pm (2i)^\mu dv_1 dw_1 dv_2 dw_2 \dots dv_\mu dw_\mu, \end{aligned}$$

где знак для нас неважен, поскольку знак вычисляемого интеграла нам известен как  $+$ . Подынтегральное выражение равно  $(\prod z_i)^{-s} = (v_1^2 + w_1^2)^{-s} (v_2^2 + w_2^2)^{-s} \dots (v_\mu^2 + w_\mu^2)^{-s}$ , а область интегрирования, которую мы обозначим через  $\mathcal{D}'$ , определяется условием  $(v_1^2 + w_1^2)(v_2^2 + w_2^2) \dots (v_\mu^2 + w_\mu^2) \geq 1$ , а также тем, что столбец  $(\log |z_1|, \log |z_2|, \dots, \log |z_\mu|) = (1/2 \log |v_1^2 + w_1^2|, 1/2 \log |v_2^2 + w_2^2|, \dots, 1/2 \log |v_\mu^2 + w_\mu^2|)$  имеет вид  $x_1 L(1 - \sigma \alpha) + x_2 L(1 - \sigma^2 \alpha) + \dots + x_\mu L(1 - \sigma^\mu \alpha)$ , где  $0 \leq x_j < 1$  (для  $j = 1, 2, \dots, \mu - 1$ , но не обязательно для  $j = \mu$ ). Значит, интеграл становится таким:

$$\frac{\pm (2i)^\mu}{\det A} \int_{\mathcal{D}'} (v_1^2 + w_1^2)^{-s} \dots (v_\mu^2 + w_\mu^2)^{-s} dv_1 dw_1 \dots dv_\mu dw_\mu.$$

Определитель, входящий в эту формулу, может быть подсчитан следующим образом.

Матрица  $A$  имеет вид  $(a_{ij})$ , где  $a_{ij} = \sigma^{i+j-1} \alpha$ , что зависит лишь от  $i + j$  по модулю  $\lambda - 1$ . Значит,  $(\lambda - 1) \times (\lambda - 1)$ -матрица  $A$  антициклическа в смысле предыдущего параграфа. Следовательно, ее определитель может быть подсчитан тем же способом, каким был подсчитан определитель матрицы  $M$  в предшествующем параграфе. Именно, можно переставить строки (или столбцы) так, чтобы матрица стала циклической, диагонализировать эту циклическую матрицу, используя базис  $(1, \rho^j, \rho^{2j}, \dots, \rho^{-j})$  ( $\rho$  — примитивный

корень  $(\lambda - 1)$ -й степени из единицы,  $j = 0, 1, \dots, \lambda - 2$ ), и заметить, что определитель есть произведение диагональных элементов. Точнее,  $\mu$  перестановок строк (первой и последней, второй и предпоследней и т. д.) приводят  $A$  к циклической матрице  $\tilde{A}$  и умножают ее определитель на  $(-1)^\mu$ . Определитель матрицы  $\tilde{A}$  есть произведение  $\lambda - 1$  чисел  $\sigma^{\lambda-1}\alpha + \rho^j\sigma\alpha + \dots + \rho^{-j}\sigma^{\lambda-2}\alpha =$   
 $= \sum_{k=0}^{\lambda-2} \rho^{jk} \sigma^k \alpha$ . Если  $j = 0$ , то это число равно  $\sigma\alpha + \sigma^2\alpha + \dots + \sigma^{\lambda-1}\alpha = \alpha + \alpha^2 + \dots + \alpha^{\lambda-1} = -1$ . Если же  $j = 1, 2, \dots, \lambda - 2$ , то оно равно  $\lambda$ , умноженному на число, которое было обозначено через  $m_j$  в формуле (2) из § 6.6. Таким образом, определитель матрицы  $A$  равен  $\pm m_1 m_2 \dots m_{\lambda-2} \cdot \lambda^{\lambda-2}$ .

Полезно также сделать следующее замечание, касающееся определителя  $\det A$ . Если антициклическую матрицу  $A$  *возвести в квадрат*, то она заметно упростится. Она превратится в матрицу  $(b_{ij})$ , для которой

$$b_{ij} = \sum_{k=1}^{\lambda-1} \sigma^{i+k-1}\alpha \sigma^{k+j-1}\alpha = \sum_{k=1}^{\lambda-1} \sigma^{i+k-1} [\alpha \sigma^{j-i}\alpha],$$

что является суммой сопряженных числа  $\alpha \cdot \sigma^{j-i}\alpha$  и равняется, следовательно,  $\lambda - 1$  при  $j - i \equiv \mu \pmod{\lambda - 1}$  и  $-1$  в остальных случаях. Таким образом,  $A^2$  циклична и ее определитель является произведением тех чисел, на которые домножаются под ее воздействием векторы  $(1, \rho^j, \rho^{2j}, \dots, \rho^{-j})$  при  $j = 0, 1, \dots, \lambda - 1$ . Если  $j = 0$ , то  $A^2$  умножает такой вектор на  $(-1) + (-1) + \dots + (-1) = \lambda - (\lambda - 1) = 1$ , в то время как при  $j = 1, 2, \dots, \lambda - 1$  она умножает его на  $-1 - \rho^j - \rho^{2j} - \dots - (\lambda - 1) \rho^{\mu j} - \dots - \rho^{-j} = -\lambda \rho^{\mu j}$ . Но  $\rho^\mu = -1$ , поэтому последнее число есть  $-\lambda$ , если  $j$  четно, и  $\lambda$ , если  $j$  нечетно. Значит,  $\det A^2 = \lambda (-\lambda) \lambda (-\lambda) \dots (-\lambda) \lambda = \pm \lambda^{\lambda-2}$ . Это дает

$$\frac{1}{\det A} = \frac{\det A}{\det A^2} = \frac{\pm m_1 m_2 \dots m_{\lambda-2} \lambda^{\lambda-2}}{\pm \lambda^{\lambda-2}} = \pm m_1 m_2 \dots m_{\lambda-2}.$$

(Как нетрудно показать, в действительности в этой формуле стоит знак  $+$  во всех случаях.)

Теперь рассмотрим замену переменных  $v_k + iw_k = e^{q_k + ir_k}$ , где  $0 < q_k < \infty$ ,  $0 \leq r_k < 2\pi$ . Тогда  $-2idv dw = (dv + idw)(dv - idw) = e^{q+ir}(dq + idr)e^{q-ir}(dq - idr) = -2ie^{2q} dq dr$ . Значит,  $dv_1 dw_1 dv_2 dw_2 \dots dv_\mu dw_\mu = \exp(2q_1 + 2q_2 + \dots + 2q_\mu) dq_1 dr_1 dq_2 dr_2 \dots dq_\mu dr_\mu$ . Подынтегральная функция превращается в произведение выражений  $(v^2 + w^2)^{-s} = e^{-2qs}$ , а область интегрирования — в множество  $\mathcal{D}''$ , для которого  $q_1 + q_2 + \dots + q_\mu \geq 0$ , вектор  $(q_1, q_2, \dots, q_\mu)$  имеет

вид  $\sum x_j L(1 - \sigma^j \alpha)$ , где  $0 \leq x_j < 1$  при  $j = 1, 2, \dots, \mu - 1$ , и  $0 \leq r_k < 2\pi$  ( $k = 1, 2, \dots, \mu$ ). Таким образом, интеграл становится равным

$$\pm (2i)^\mu m_1 m_2 \dots m_{\lambda-2} \int_{\mathcal{Z}''} e^{(2-2s)(q_1+q_2+\dots+q_\mu)} dq_1 dr_1 dq_2 dr_2 \dots dq_\mu dr_\mu.$$

Перенесем все  $r_j$ ,  $j = 1, \dots, \mu$ , в конец и проинтегрируем по ним. Получим

$$\pm (2i)^\mu (2\pi)^\mu m_1 m_2 \dots m_{\lambda-2} \int_{\mathcal{Z}'''} e^{(2-2s)(q_1+q_2+\dots+q_\mu)} dq_1 dq_2 \dots dq_\mu,$$

где через  $\mathcal{Z}'''$  обозначена проекция области  $\mathcal{Z}''$  на пространство  $q$ -координат.

Наконец, рассмотрим замену координат, неявно определенную равенством  $q = Mx$ , где  $q$  — вектор-столбец  $(q_1, q_2, \dots, q_\mu)$ ,  $x$  — вектор-столбец  $(x_1, x_2, \dots, x_\mu)$  и  $M$  — антициклическая  $\mu \times \mu$ -матрица  $(\log |1 - \sigma^{i+j-1} \alpha|)$  из предыдущего параграфа. Тогда, по определению области  $\mathcal{Z}'''$ , область интегрирования относительно переменных  $x$  состоит попросту из тех  $x$ , лежащих в  $\mathcal{S}$ , которые соответствуют точкам  $(q_1, q_2, \dots, q_\mu)$ , удовлетворяющим условию  $q_1 + q_2 + \dots + q_\mu \geq 0$ . В предыдущем параграфе отмечалось, что так как суммы элементов матрицы  $M$  по столбцам все равны  $1/2 \log \lambda$ , то  $q_1 + q_2 + \dots + q_\mu = 1/2 (\log \lambda) (x_1 + x_2 + \dots + x_\mu)$ . Следовательно интеграл принимает вид

$$\pm (2i)^\mu (2\pi)^\mu m_1 m_2 \dots m_{\lambda-2} \det M \times \\ \times \int_{\substack{x \in \mathcal{S} \\ x_1 + x_2 + \dots + x_\mu \geq 0}} e^{(1-s)(\log \lambda)(x_1 + x_2 + \dots + x_\mu)} dx_1 dx_2 \dots dx_\mu.$$

Введем новую переменную  $t = x_1 + x_2 + \dots + x_\mu$  и проинтегрируем по переменным  $x_1, x_2, \dots, x_{\mu-1}$ . Тогда у нас останется тот же сомножитель, умноженный на интеграл

$$\int_{\geq 0} \exp [(1-s)(\log \lambda)t] dt = [(s-1) \log \lambda]^{-1}.$$

Следовательно, значение искомой величины (1) равно

$$\pm (4\pi i)^\mu m_1 m_2 \dots m_{\lambda-2} \frac{\det M}{(s-1) \log \lambda}.$$

В предыдущем параграфе было показано, что  $\det \hat{M} = (\log \sqrt{\lambda}) C_1 C_2 \dots C_{\mu-1}$ . Поскольку  $M$  и  $\hat{M}$  отличаются только

порядком строк, имеем  $\det M = \pm \det \tilde{M}$ . Таким образом, интеграл (1) равен абсолютной величине выражения

$$\pm 2^{2\mu-1}(\pi i)^\mu m_1 m_2 \dots m_{\lambda-2} C_1 C_2 \dots C_{\mu-1} (s-1)^{-1}.$$

Этим заканчивается вычисление интеграла.

## 6.12. Сравнение интеграла с суммой

Пусть  $I(s)$  и  $S(s)$  обозначают рассматриваемые нами интеграл и сумму, т. е.

$$I(s) = \int_{\mathcal{D}} N(u_1 \sigma \alpha + \dots + u_{\lambda-1} \sigma^{\lambda-1} \alpha)^{-s} du_1 du_2 \dots du_{\lambda-1},$$

$$S(s) = \sum_{\mathcal{D}} N g(\alpha)^{-s}.$$

Мы уже показали, что сумма сходится при всех  $s > 1$  и что предел  $\lim (s-1) S(s)$  при  $s \downarrow 1$  существует. Сейчас нам нужно показать, что при всех  $s > 1$  интеграл тоже сходится и при  $s \downarrow 1$  произведение  $(s-1) I(s)$  имеет предел, который равен пределу произведения  $(s-1) S(s)$ .

Для того чтобы установить эти факты, полезно изменить множество  $\mathcal{P} = \{(x_1, \dots, x_\mu): 0 \leq x_1 < 1, \dots, 0 \leq x_{\mu-1} < 1, x_\mu \text{ не ограничено}\}$ , при помощи которого была определена область  $\mathcal{D}$ . Это делается по следующей причине. При оценке значений  $I(s)$  и  $S(s)$  удобно рассматривать изменения масштаба  $(u_1, u_2, \dots, u_{\lambda-1}) \rightarrow (cu_1, cu_2, \dots, cu_{\lambda-1})$  в пространстве переменных  $u_1, u_2, \dots, u_{\lambda-1}$ , а область  $\mathcal{D}$ , как она определялась ранее, не инвариантна относительно изменений масштаба. В качестве первого шага нашего доказательства будет дано определение новой области  $\mathcal{D}'$ , относительно которой и интеграл и сумма не изменяются, но для которой будет значительно легче производить изменения масштаба.

Мы выбирали область  $\mathcal{P}$ , руководствуясь следующим свойством: для любой заданной точки  $(x_1, x_2, \dots, x_\mu)$  в пространстве переменных  $x_1, x_2, \dots, x_\mu$  имеется точно один способ выбора таких целых чисел  $n_1, n_2, \dots, n_\mu$ , что  $n_1 + n_2 + \dots + n_\mu = 0$  и точка  $(x_1 + n_1, x_2 + n_2, \dots, x_\mu + n_\mu)$  лежит в  $\mathcal{P}$ . Изменению масштаба в пространстве переменных  $u_1, u_2, \dots, u_{\lambda-1}$  соответствует под действием функции  $\Phi$  сложение с вектором, коллинеарным вектору  $(1, 1, \dots, 1)$  в пространстве переменных  $x_1, x_2, \dots, x_\mu$ . Этим и обусловлено введение множества  $\mathcal{P}'$  с теми же свойствами, что и  $\mathcal{P}$ , но инвариантного относительно переноса на векторы, коллинеарные вектору  $(1, 1, \dots, 1)$ . Конкретнее, пусть  $\mathcal{P}'$  — множество всех точек пространства переменных  $x_1, x_2, \dots$

$\dots, x_\mu$ , для которых  $0 \leq x_j - \mu^{-1}(x_1 + x_2 + \dots + x_\mu) < 1$  при  $j = 1, 2, \dots, \mu - 1$ . Тогда множества  $\mathcal{S}$  и  $\mathcal{S}'$  состоят из одних и тех же точек, для которых  $x_1 + x_2 + \dots + x_\mu = 0$ , но  $\mathcal{S}'$  инвариантно относительно сложения с векторами, коллинеарными вектору  $(1, 1, \dots, 1)$  (прибавление вектора  $c(1, 1, \dots, 1)$  к  $(x_1, x_2, \dots, x_\mu)$  сводится к прибавлению числа  $c$  и к координатам  $x_j$ , и к их среднему арифметическому  $\mu^{-1}(x_1 + x_2 + \dots + x_\mu)$ , а поэтому оставляет величину  $x_j - \mu^{-1}(x_1 + x_2 + \dots + x_\mu)$  неизменной), тогда как  $\mathcal{S}$  инвариантно относительно сложения с векторами, коллинеарными вектору  $(0, 0, \dots, 0, 1)$ .

Пусть  $\mathcal{Q}'$  — множество точек в пространстве переменных  $u_1, u_2, \dots, u_{\lambda-1}$ , для которых выполняется условие  $Ng(\alpha) \geq 1$  и  $\Phi$ -образ которых лежит в  $\mathcal{S}'$ . Легко доказать, что  $\mathcal{S}'$  обладает тем же свойством, что и описанное ранее множество  $\mathcal{S}$ . Отсюда следует, что для каждого кругового целого  $g(\alpha)$  имеется точно один способ выбора таких целых чисел  $n_1, n_2, \dots, n_\mu$ , что  $n_1 + n_2 + \dots + n_\mu = 0$  и  $(1 - \sigma\alpha)^{n_1} (1 - \sigma^2\alpha)^{n_2} \dots (1 - \sigma^\mu\alpha)^{n_\mu} g(\alpha)$  лежит в  $\mathcal{Q}'$ . Поэтому

$$S(s) = \sum_{g(\alpha) \in \mathcal{Q}'} Ng(\alpha)^{-s},$$

ибо обе части этого равенства равны  $2\lambda h_2 \sum N(A)^{-s}$ , где  $A$  пробегает все главные дивизоры. В то же время

$$I(s) = \int_{\mathcal{Q}'} N(u_1\sigma\alpha + \dots + u_{\lambda-1}\sigma^{\lambda-1}\alpha)^{-s} du_1 du_2 \dots du_{\lambda-1}.$$

В этом легче всего убедиться, если проследить вычисление интеграла  $I(s)$  в предыдущем параграфе и заметить, что все рассуждения применимы к области  $\mathcal{Q}'$  точно так же, как и к  $\mathcal{Q}$ , за исключением последнего этапа, когда нужно интегрировать выражение

$$e^{(1-s) \log \lambda (x_1 + x_2 + \dots + x_\mu)} dx_1 dx_2 \dots dx_\mu$$

по области  $\mathcal{S}'$  вместо  $\mathcal{S}$ . Значение этого интеграла в обоих случаях равно  $[(s-1) \log \lambda]^{-1}$ , что можно проверить, применив замену переменных  $y_1 = x_1, \dots, y_{\mu-1} = x_{\mu-1}, t = x_1 + x_2 + \dots + x_\mu$  в случае области  $\mathcal{S}$  и замену  $y_1 = x_1 - \mu^{-1}t, y_2 = x_2 - \mu^{-1}t, \dots, y_{\mu-1} = x_{\mu-1} - \mu^{-1}t, t = x_1 + x_2 + \dots + x_\mu$  в случае области  $\mathcal{S}'$ .

Пусть область  $\mathcal{Q}'$  разбита на области  $\mathcal{Q}_0 = \{(u) \in \mathcal{Q}': 1 \leq Nu < 2^{\lambda-1}\}, \mathcal{Q}_1 = \{(u) \in \mathcal{Q}': 2^{\lambda-1} \leq Nu < 4^{\lambda-1}\}, \dots, \mathcal{Q}_k = \{(u) \in \mathcal{Q}': 2^{k(\lambda-1)} \leq Nu < 2^{(k+1)(\lambda-1)}, \dots\}$ , или, что то же самое (поскольку область  $\mathcal{Q}'$  инвариантна относительно изменений масштаба),  $\mathcal{Q}_k = \{(u) \in \mathcal{Q}': (2^{-k}u) \in \mathcal{Q}_0\}$ . Здесь использованы обозначения:  $(u) = (u_1, u_2, \dots, u_{\lambda-1}), (2^{-k}u) = (2^{-k}u_1, 2^{-k}u_2, \dots$

$\dots, 2^{-k}u_{\lambda-1})$ ,  $Nu$  — произведение всех  $\lambda - 1$  сопряженных числа  $u_1\sigma\alpha + u_2\sigma^2\alpha + \dots + u_{\lambda-1}\sigma^{\lambda-1}\alpha$ . Пусть равенства  $S(s) = S_0(s) + S_1(s) + S_2(s) + \dots$  и  $I(s) = I_0(s) + I_1(s) + I_2(s) + \dots$  представляют собой соответствующие разбиения суммы  $S(s)$  и интеграла  $I(s)$ . Иными словами, пусть  $S_k(s)$  — сумма значений  $Ng(\alpha)^{-s}$  по всем круговым целым из  $\mathcal{D}_k$ , и пусть  $I_k(s)$  — интеграл от  $N(u_1\sigma\alpha + \dots + u_{\lambda-1}\sigma^{\lambda-1}\alpha)^{-s} du_1 du_2 \dots du_{\lambda-1}$  по области  $\mathcal{D}_k$ . Поскольку сумма  $S(s)$  сходится абсолютно (как ряд с положительными членами), можно суммировать в предлагаемом порядке:  $S(s) = S_0(s) + S_1(s) + \dots$ . Для доказательства сходимости несобственного интеграла  $I(s)$  при  $s > 1$  достаточно доказать, что имеется такой сходящийся ряд  $\delta_0(s) + \delta_1(s) + \delta_2(s) + \dots$ , что  $|S_k(s) - I_k(s)| < \delta_k(s)$ , поскольку это дает:  $I_m(s) + I_{m+1}(s) + \dots + I_n(s) \leq S_m(s) + |\delta_m(s)| + S_{m+1}(s) + |\delta_{m+1}(s)| + \dots + S_n(s) + |\delta_n(s)|$ , т. е.  $I(s)$  удовлетворяет критерию Коши. Если, кроме того, доказано, что при  $s \downarrow 1$  члены  $\delta_k(s)$  ограничены членами сходящегося ряда констант  $\delta_0 + \delta_1 + \delta_2 + \dots$ , то отсюда будет следовать, что величина  $|S(s) - I(s)|$  остается ограниченной при  $s \downarrow 1$ , т. е. предел  $\lim (s - 1) I(s) = \lim [(s - 1) S(s) + (s - 1) (I(s) - S(s))]$  существует и равен  $\lim (s - 1) S(s) + 0$ , а нам это и нужно. Таким образом, нужная нам теорема будет доказана, если будут найдены такие оценки  $|S_k(s) - I_k(s)| < \delta_k(s)$ , что  $\sum \delta_k(s) < \infty$ , причем чтобы для  $1 < s \leq 2$  мы имели  $\delta_k(s) < \delta_k$ , где  $\sum \delta_k < \infty$ . Конечно, при доказательстве этих утверждений можно пренебречь любым конечным числом начальных членов ряда (ибо как  $S_k(s)$ , так и  $I_k(s)$  сходятся при  $s > 1$  и оба они ограничены при  $s \downarrow 1$ ). Значит, мы можем сосредоточиться на оценке величины  $|S_k(s) - I_k(s)|$  для больших номеров  $k$ .

Пусть пространство переменных  $u_1, u_2, \dots, u_{\lambda-1}$  разделено на «кубы» вида  $\{(u): |u_j - n_j| \leq 1/2\}$  с единичным ребром, имеющие центры в точках  $(n_1, n_2, \dots, n_{\lambda-1})$ , все координаты которых целые. Для данного целого числа  $k$  разность  $S_k(s) - I_k(s)$  можно записать как сумму слагаемых по всем кубам, причем каждое слагаемое представляет собой разность между членом суммы  $S_k(s)$ , являющимся значением нормы  $Ng(\alpha)^{-s}$  в центре этого куба (если такой существует), и частью интеграла  $I_k(s)$ , взятой по этому кубу, если таковая имеется. Могут встретиться три типа кубов:

- (i) кубы, не содержащие точек из  $\mathcal{D}_k$ ;
- (ii) кубы, целиком содержащиеся в  $\mathcal{D}_k$ ;
- (iii) кубы, лежащие на границе области  $\mathcal{D}_k$ , т. е. содержащие как точки изнутри  $\mathcal{D}_k$ , так и точки извне  $\mathcal{D}_k$ .

Конечно, для кубов типа (i) соответствующие части как  $S_k(s)$ , так и  $I_k(s)$ , обе равны нулю, а значит, и их разность равна нулю.



Остается оценить полную разность между  $S_k(s)$  и  $I_k(s)$  по всем кубам типов (ii) и (iii). Оценки для этих двух типов кубов совершенно различны, и естественно их разделить. Оценка для кубов типа (iii) легче, с нее мы и начнем.

Член суммы  $S_k(s)$ , соответствующий кубу типа (iii), равен 0 или  $N^{-s}$ , поэтому он не превосходит числа  $[2^{k(\lambda-1)}]^{-s} \leq 2^{-k(\lambda-1)}$ . Сходным образом, часть интеграла  $I_k(s)$ , соответствующая такому кубу, не больше чем  $2^{-k(\lambda-1)}$ . Разность двух положительных чисел по абсолютной величине не превосходит большего из них, поэтому часть величины  $|S_k(s) - I_k(s)|$ , соответствующая кубам типа (iii), не превосходит числа  $2^{-k(\lambda-1)}$ , умноженного на количество таких кубов (для всех  $s > 1$ ). Но число таких кубов равно числу кубов, лежащих на границе области  $\mathcal{Q}_0$ , когда пространство переменных  $u_1, u_2, \dots, u_{\lambda-1}$  разделено на кубы с ребром  $2^{-k}$ . Поэтому задача свелась к оценке числа этих кубов. Такая оценка очень важна в теории интегрирования по областям, подобным области  $\mathcal{Q}_0$ . Используя тот факт, что граница области  $\mathcal{Q}_0$  компактна и невырожденна, легко доказать (см. упр. 1), что число таких кубов не превосходит константы, умноженной на  $(2^k)^{\lambda-2}$ . Следовательно, часть величины  $|S_k(s) - I_k(s)|$ , соответствующая кубам типа (iii), не больше константы, умноженной на  $2^{k(\lambda-2)} 2^{-k(\lambda-1)} = 2^{-k}$  для всех  $s \geq 1$ . Поскольку  $\sum 2^{-k} < \infty$ , этим доказана искомая оценка для кубов типа (iii).

Теперь рассмотрим кубы типа (ii). Пусть  $N_c^{-s}$  — значение нормы  $N^{-s}$  в центре куба. Тогда, поскольку объем куба равен 1, член суммы  $S_k(s)$ , соответствующий этому кубу, может быть записан как интеграл от постоянной функции  $N_c^{-s}$  по кубу, а часть величины  $|S_k(s) - I_k(s)|$ , соответствующая этому кубу, не больше интеграла от  $|N^{-s} - N_c^{-s}|$  по кубу. Последний в свою очередь не превосходит максимума величины  $|N^{-s} - N_c^{-s}|$  на кубе. Значит, естественно искать оценку величины  $|N^{-s} - N_c^{-s}|$ . Согласно основной теореме интегрального исчисления, величина  $N^{-s} - N_c^{-s}$  равна интегралу вдоль пути внутри куба от его центра до некоторой его точки от выражения  $d(N^{-s}) = (-s) N^{-s} (dN/N)$ . Значение величины  $N^{-s}$  примерно равно  $N_c^{-s}$ : их отношение  $N^{-s}/N_c^{-s}$  не превосходит  $[2^{k(\lambda-1)}]^s/[2^{(k+1)(\lambda-1)}]^s = 2^{-s(\lambda-1)} < 2^{-(\lambda-1)}$ . Таким образом,  $|(-s) N^{-s}|$  меньше константы, умноженной на  $N_c^{-s}$ , причем эта константа не зависит от  $s$ . Дифференциальная форма  $dN/N$  инвариантна относительно изменений масштаба ( $N$  — однородный полином от  $u_1, u_2, \dots, u_{\lambda-1}$ ), а отсюда легко следует, что интеграл от этой формы по пути, идущему из центра в другую точку куба, ограничен одним и тем же числом для всех кубов типа (ii). (В действительности, как будет показано чуть ниже, эта граница стремится к нулю при  $k \rightarrow \infty$ .) Таким образом, часть разности  $S_k(s) - I_k(s)$ , соответствующая этому кубу, не превосходит константы, умноженной на  $N_c^{-s}$ , а полная разность не превосходит

константы, умноженной на  $S_k(s)$ . Такой оценки достаточно, чтобы доказать сходимость интеграла  $I(s)$ , поскольку  $\sum S_k(s) < \infty$ . Однако при  $s \downarrow 1$  это не дает равномерной границы для  $|S(s) - I(s)|$ , поскольку ряд  $\sum S_k(s) = S(s)$  стремится к ряду  $\sum N^{-1}$ , который расходится. Поэтому требуется более тонкая оценка, которая принимала бы во внимание тот факт, что интеграл от  $dN/N$  мал.

Как мы раньше заметили, интеграл от  $dN/N$  между двумя точками куба типа (ii) равен интегралу от  $dN/N$  между образами этих двух точек после изменения масштаба  $(u) \mapsto (2^{-k}u)$ . (Заметим, что  $dN/N = d \log N$  является замкнутой дифференциальной формой, так что этот интеграл не зависит от пути.) Но эти две точки лежат в  $\mathcal{D}_0$ , и их координаты разнятся не более чем на  $2^{-k}$  во всех  $\lambda - 1$  координатных направлениях. Так как область  $\mathcal{D}_0$  ограничена, а функция  $\log N$  непрерывно дифференцируема на ее замыкании, то частные производные от  $\log N$  ограничены на  $\mathcal{D}_0$ , а отсюда легко следует, что рассматриваемый интеграл не превосходит константы, умноженной на  $2^{-k}$ . Поскольку  $N_c \leq 2^{(k+1)(\lambda-1)}$ ,  $N_c^{1/(\lambda-1)} \leq 2^{k+1}$ ,  $2N_c^{-1/(\lambda-1)} \geq 2^{-k}$ , сумма по всем таким кубам не превосходит константы, умноженной на  $\sum N_c^{-t}$ , где  $t = 1 + (\lambda - 1)^{-1}$ . Эта оценка имеет место для  $s \geq 1$ , и, поскольку  $\sum N_c^{-t}$  — сходящийся ряд, наше доказательство завершено.

## Упражнение

1. Докажите, что если пространство переменных  $u_1, u_2, \dots, u_{\lambda-1}$  разделено на «кубы» с ребром  $2^{-k}$ , то имеется такая постоянная  $B$ , что общее число кубов на границе области  $\mathcal{D}_0$  не превосходит  $B \cdot 2^{k(\lambda-2)}$  для  $k = 1, 2, \dots$ . [Докажите вначале, что граница области  $\mathcal{D}_0$  компактна и невырожденна в том смысле, что она может быть представлена как образ конечного числа (возможно, перекрывающихся) непрерывно дифференцируемых неособых отображений  $(\lambda - 2)$ -мерного куба. В действительности  $\Phi$ -образ области  $\mathcal{D}_0$  есть куб в пространстве переменных  $x_1, x_2, \dots, x_\mu$ , и с использованием отображений из предыдущего параграфа можно дать явные параметризации границы области  $\mathcal{D}_0$ . По теореме о неявной функции, отсюда следует, что локально граница области  $\mathcal{D}_0$  может быть параметризована посредством  $\lambda - 2$  из  $\lambda - 1$  координатных функций в пространстве переменных  $u_1, u_2, \dots, u_{\lambda-1}$ . Для каждого так параметризованного участка число кубов с ребром  $2^{-k}$ , которые он может пересекать, равно константе, умноженной на число кубов в  $(\lambda - 2)$ -мерной координатной плоскости, над которыми он лежит, причем константа появляется из-за верхних границ частных производных параметризующей функции. Разумеется, число кубов в координатной плоскости меньше константы, умноженной на  $2^{k(\lambda-2)}$ . Так как вся граница покрыта конечным числом таких участков, то отсюда следует требуемая оценка.]

### 6.13. Сумма по другим классам дивизоров

В § 6.2 отмечалось, что сумма значений  $N(A)^{-s}$  по любым двум классам дивизоров в пределе при  $s \downarrow 1$  одинакова. Иными словами,

$$\lim_{s \downarrow 1} \left[ \sum_{A \sim B} N(A)^{-s} / \sum_{A \sim I} N(A)^{-s} \right] = 1, \quad (1)$$

где  $B$  — данный дивизор, сумма в числителе распространяется на все дивизоры, эквивалентные  $B$ , а суммирование в знаменателе происходит по всем главным дивизорам. Этот факт, отчетливо предсказываемый формулой Дирихле для числа классов в квадратичном случае, может быть доказан следующим образом.

Пусть  $B$  — данный дивизор, а  $C$  — такой дивизор, что  $BC \sim I$ . Тогда из  $A \sim B$  вытекает  $AC \sim I$ , т. е.  $A' = AC$  является главным дивизором, делящимся на  $C$ . Обратно, если  $A'$  — главный дивизор, делящийся на  $C$ , например  $A' = AC$ , то частное  $A$  удовлетворяет условию  $A \sim ABC = A'B \sim IB \sim B$ . Это означает, что отображение  $A \mapsto AC$  устанавливает взаимно однозначное соответствие между дивизорами  $A$ , эквивалентными дивизору  $B$ , и главными дивизорами  $A'$ , делящимися на  $C$ . Из  $N(A') = N(AC) = N(A)N(C)$  следует, что

$$\sum_{A \sim B} N(A)^{-s} = \sum_{A \sim B} N(C)^s N(AC)^{-s} = N(C)^s \sum_{\substack{A' \sim I \\ C \mid A'}} N(A')^{-s}.$$

Следовательно, доказываемое утверждение можно переформулировать так:

$$\lim_{s \downarrow 1} \left[ N(C)^s \sum_{\substack{A' \sim I \\ C \mid A'}} N(A')^{-s} / \sum_{A \sim I} N(A)^{-s} \right] = 1.$$

Поскольку  $\lim N(C)^s = N(C)$ , это является утверждением о том, что в пределе при  $s \downarrow 1$  сумма  $\sum N(A)^{-s}$  по *всем* главным дивизорам равна числу  $N(C)$ , умноженному на такого же типа сумму, но только по тем главным дивизорам, которые делятся на  $C$ . Теперь заметим, что  $N(C)$  — положительное целое число, и поэтому, говоря нестрого, доказываемое утверждение является попросту утверждением о том, что *одно из каждой  $N(C)$  круговых целых делится на  $C$* .

Более точно, рассмотрим задачу вычисления в пределе при  $s \downarrow 1$  суммы  $\sum N(A)^{-s}$  по всем главным дивизорам  $A$ , делящимся на данный дивизор  $C$ . Если  $L$  обозначает множество всех круговых целых, делящихся на  $C$ , то ясно, что, как и в уже рассмотренном случае  $C = I$ , при  $s > 1$

$$\sum_{\substack{A \text{ главный} \\ C \mid A}} N(A)^{-s} = \frac{1}{2\lambda h_2} \sum_{\substack{\Phi(g(\alpha)) \in \mathcal{D} \\ g(\alpha) \in L}} N g(\alpha)^{-s}.$$

Иными словами, для каждого главного дивизора  $A$ , делящегося на  $C$ , имеется точно  $2\lambda h_2$  круговых целых  $g(\alpha)$ , дивизор которых есть  $A$  и  $\Phi$ -образы которых лежат в  $\mathcal{D}$ .

Пусть теперь пространство переменных  $u_1, u_2, \dots, u_{\lambda-1}$  разделено на «кубы» с вершинами в точках, все координаты которых являются целыми числами, делящимися на  $N(C)$ . Вершины этих кубов все лежат в  $L$ , поскольку из делимости на  $N(C)$  вытекает делимость на  $C$ . Тогда на основании рассуждений из предыдущего параграфа получаем

$$\begin{aligned} \lim_{s \downarrow 1} (s-1) \int_{\mathcal{D}} N(u_1 \sigma \alpha + \dots + u_{\lambda-1} \sigma^{\lambda-1} \alpha) du_1 \dots du_{\lambda-1} = \\ = \lim_{s \downarrow 1} (s-1) \sum_{\substack{\text{по кубам} \\ \text{в } \mathcal{D}}} N(\text{точка куба})^{-s} (\text{объем куба}). \end{aligned}$$

Здесь можно пренебречь изменением величины  $N^{-s}$  в каждом кубе, а также суммой по всем тем кубам, которые входят в  $\mathcal{D}$  лишь частично.

Пусть каждая точка  $(u_1, u_2, \dots, u_{\lambda-1})$  из  $L$  поставлена в соответствие тому кубу, который содержит точки  $(u_1 + \varepsilon, u_2 + \varepsilon, \dots, u_{\lambda-1} + \varepsilon)$  при всех достаточно малых  $\varepsilon$ . Тогда каждому кубу отвечает одинаковое число (обозначим его через  $\nu$ ) точек из  $L$ , поскольку точка  $(u_1, u_2, \dots, u_{\lambda-1})$  тогда и только тогда лежит в  $L$ , когда точка  $(u_1 + n_1 N(C), u_2 + n_2 N(C), \dots, u_{\lambda-1} + n_{\lambda-1} N(C))$  лежит в  $L$  при любых целых  $n_1, n_2, \dots, n_{\lambda-1}$ . В написанной выше сумме по кубам можно использовать в качестве значения  $N^{-s}$  среднее из значений  $N g(\alpha)^{-s}$  по  $\nu$  точкам из  $L$ , отвечающих данному кубу. Тогда долей каждого куба, лежащего внутри  $\mathcal{D}$ , в рассматриваемой сумме будет слагаемое

$$\frac{N g_1(\alpha)^{-s} + N g_2(\alpha)^{-s} + \dots + N g_\nu(\alpha)^{-s}}{\nu} N(C)^{\lambda-1},$$

где  $g_1(\alpha), g_2(\alpha), \dots, g_\nu(\alpha)$  — все  $\nu$  точек из  $L$ , отвечающих этому кубу. Отсюда видно, что предел данной суммы равен

$$\lim_{s \downarrow 1} (s-1) \frac{N(C)^{\lambda-1}}{\nu} \sum_{\substack{g(\alpha) \in \mathcal{D} \\ g(\alpha) \in L}} N g(\alpha)^{-s}.$$

С другой стороны, предел интеграла, стоящего в левой части равенства, также имеет вид

$$\lim_{s \downarrow 1} (s-1) \sum_{\mathcal{D}} N g(\alpha)^{-s},$$

что равно числу  $2\lambda h_2$ , умноженному на сумму значений  $N(A)^{-s}$  по всем главным дивизорам. Следовательно,

$$\frac{N(C)^{\lambda-1}}{v} \lim_{s \downarrow 1} (s-1) \sum_{\substack{A \sim I \\ C \mid A}} N(A)^{-s} = \lim_{s \downarrow 1} (s-1) \sum_{A \sim I} N(A)^{-s},$$

и утверждение, которое доказывается, принимает вид

$$\frac{N(C)^{\lambda-1}}{v} = N(C).$$

А это — чисто арифметическое утверждение, в которое не входят пределы и бесконечные суммы. Его можно очень просто доказать так.

Как было показано в § 4.14, норма  $N(C)$  равна числу классов сравнения по модулю  $C$ . Так как  $N(C)^{\lambda-1}$  равно числу круговых целых в кубе с ребром  $N(C)$ , то искомое равенство  $N(C)^{\lambda-1} = v \cdot N(C)$  будет доказано, если мы покажем, что каждый из  $N(C)$  классов сравнения содержит точно по  $v$  круговых целых в каждом кубе. Если  $g(\alpha)$  — некоторое круговое целое, то с ним сравнимы по модулю  $C$  те круговые целые, которые представимы в виде  $g(\alpha) + h(\alpha)$ , где  $h(\alpha)$  делится на  $C$ . Иными словами, в пространстве переменных  $u_1, u_2, \dots, u_{\lambda-1}$  точки, соответствующие круговым целым в данном классе сравнения  $\{g(\alpha) + h(\alpha)\}$  по модулю  $C$ , составляют *сдвиг* множества  $L$  точек, соответствующих делящимся на  $C$  круговым целым. Значит, достаточно доказать, что  $L$  обладает тем свойством, что в любом его сдвиге имеется столько же точек данного куба с ребром  $N(C)$ , сколько и в самом  $L$ . Очевидно, что это верно для сдвигов на 1 вдоль любого из координатных направлений, поскольку каждой точке, выходящей из куба на одном конце направления, соответствует точка, входящая в куб на противоположном конце. Но каждый сдвиг есть композиция сдвигов на 1 вдоль координатных направлений, и, значит, этим завершено доказательство утверждения (1).

## 6.14. Формула числа классов

Пусть  $h$  — число классов эквивалентности дивизоров. На основании доказанного в предыдущем параграфе утверждения о том, что предел  $\lim (s-1) \sum N(A)^{-s}$  одинаков при суммировании по любому классу, мы можем утверждать, что  $\lim (s-1) \sum N(A)^{-s}$ , где суммирование происходит по *всем* классам, равен числу  $h$ , умноженному на предел  $\lim (s-1) \sum' N(A)^{-s}$ , где суммирование распространено на главный класс. Значит, если фор-

мулу эйлерова произведения

$$\sum_{\substack{\text{все} \\ \text{дивизоры } A}} N(A)^{-s} = \prod_{\substack{\text{все} \\ \text{простые} \\ \text{дивизоры } P}} (1 - N(P)^{-s})^{-1}$$

умножить на  $(s-1)$ , то в пределе при  $s \downarrow 1$ , как было выше найдено, мы получим

$$\begin{aligned} & \pm h \frac{1}{2\lambda h_2} 2^{2\mu-1} (\pi i)^\mu m_1 m_2 \dots m_{\lambda-2} C_1 C_2 \dots C_{\mu-1} = \\ & = (-2)^{\mu-1} \left( \frac{i\pi}{\lambda} \right)^\mu m_1 m_2 \dots m_{\lambda-2} C_1 C_2 \dots C_{\mu-1} \varphi(\beta) \varphi(\beta^3) \dots \varphi(\beta^{\lambda-2}), \end{aligned}$$

что приводится к виду

$$h = \pm \frac{\varphi(\beta) \varphi(\beta^3) \dots \varphi(\beta^{\lambda-2})}{(2\lambda)^{\mu-1}} \cdot h_2.$$

Это и есть *формула числа классов*, причем, по существу, в той же форме, в которой она была дана Куммером.

Число классов здесь выступает в виде произведения двух сомножителей, которые традиционно называют *первый сомножитель* и *второй сомножитель* числа классов. Вторым сомножителем  $h_2$  является положительным целым числом; он был определен в § 6.10. Вкратце его смысл таков:  $h_2$  — это число единиц  $E_j$ , которые необходимы, чтобы можно было любую круговую единицу записать в виде

$$\pm \alpha^k E_j (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$$

при некотором выборе знака, показателя  $k = 1, 2, \dots, \lambda$ , индекса  $j = 1, 2, \dots, h_2$  и целых чисел  $x_1, x_2, \dots, x_\mu$ , удовлетворяющих условию  $x_1 + x_2 + \dots + x_\mu = 0$ . (В терминах теории групп  $h_2$  — индекс группы единиц вида  $\pm \alpha^k \prod (1 - \sigma^v\alpha)^{x_v}$  в группе всех единиц.) Первый сомножитель, который обозначают также через  $h_1$ ,

$$h_1 = \pm \frac{\varphi(\beta) \varphi(\beta^3) \dots \varphi(\beta^{\lambda-2})}{(2\lambda)^{\mu-1}},$$

в действительности является целым числом. Конечно, знак выбирается так, чтобы это число оказалось положительным. Напомним, что  $\beta$  — примитивный корень  $(\lambda-1)$ -й степени из единицы, а  $\varphi(X)$  есть, по определению, полином  $\varphi(X) = 1 + \gamma X + \gamma_2 X^2 + \dots + \gamma_{\lambda-2} X^{\lambda-2}$ , где  $0 < \gamma_j < \lambda$ ,  $\gamma = \gamma_1$  — примитивный корень по модулю  $\lambda$  и  $\gamma_j \equiv \gamma^j \pmod{\lambda}$ . Итак, в отличие от  $h_2$  сомножитель  $h_1$  задается явной формулой, все члены которой простым образом зависят от  $\lambda$ . В следующем параграфе будет доказано, что  $2^{\mu-1} h_1$  — целое число. Нетрудно доказать, что  $h_1$  само есть целое



число (см. упр. 2 к § 6.15), как и утверждал Куммер, но нам это не понадобится.

Куммер использовал для обозначения произведения  $\varphi(\beta)\varphi(\beta^3)\dots\varphi(\beta^{\lambda-2})$  букву  $P$ , так что формула числа классов принимает вид

$$h = \frac{|P|}{(2\lambda)^{\mu-1}} \cdot h_2.$$

Он также дал описание целого числа  $h_2$  как частного двух определителей  $h_2 = D/\Delta$ , но числитель  $D$  фактически нельзя найти, не выяснив структуру группы единиц до такой степени, что уже станет возможным найти само  $h_2$ . Поэтому прямое описание числа  $h_2$  лучше, чем это частное определителей. В любом случае вычисление сомножителя  $h_2$  значительно труднее вычисления сомножителя  $h_1$ . К счастью, как будет видно в следующих параграфах, для того чтобы доказать Последнюю теорему Ферма для данного  $\lambda$ , т. е. для того чтобы доказать, что выполняются (А) и (В), совсем не требуется вычислять ни  $h_1$ , ни  $h_2$ . В этом и заключается большое удобство критерия Куммера, сформулированного в терминах числителей чисел Бернулли.

## Упражнение

1. Докажите прямым подсчетом, что первый сомножитель числа классов для  $\lambda = 3, 5, 7, 11, 13$  равен 1. Определите знак произведения  $\varphi(\beta)\varphi(\beta^3)\dots\varphi(\beta^{\lambda-2})$  в каждом из этих случаев.

## 6.15. Доказательство иррегулярности числа 37

Формула  $\pm P/(2\lambda)^{\mu-1}$  для первого сомножителя числа классов предписывает вполне определенные алгебраические выкладки, которые при малых значениях  $\lambda$  можно выполнить и найти это число (см. упр. 1 к предыдущему параграфу). Случай  $\lambda = 37$  не лежит вне достижимости этих выкладок, и Куммер в конце концов вычислил <sup>1)</sup> не только этот сомножитель — найдя, что он равен 37, — но также первый сомножитель числа классов для всех простых чисел  $\lambda < 100$ . Какая часть этих вычислений была завершена в течение лета 1847 г., неизвестно, но из того, что известно о методах работы Куммера, кажется, вполне можно сказать, что к тому времени он уже много занимался вычислением конкретных чисел классов. Во всяком случае, благодаря ли богатому вычислительному опыту или в результате прямого вдохновения, но в 1847 г. ему удалось открыть искусные приемы для решения того

<sup>1)</sup> См. [К14, стр. 473]. Куммер позже говорил (см. [К15, стр. 199]) что эти вычисления были выполнены «не без больших усилий». Он также внес исправления в случай  $\lambda = 71$ . В [К17] Куммер довел эти вычисления до  $\lambda = 163$  и сделал несколько элементарных замечаний о способе счета.

частного вопроса о числе  $P/(2\lambda)^{\mu-1}$ , который его больше всего интересовал, а именно узнать, делится ли оно на  $\lambda$ , не производя фактического вычисления. Этот параграф посвящен доказательству того, что в частном случае  $\lambda = 37$  ответ таков:  $\lambda$  действительно делит первый сомножитель числа классов. В следующем параграфе будет показано, как можно использовать ту же технику для установления необходимого и достаточного условия делимости числа  $P/(2\lambda)^{\mu-1}$  на  $\lambda$ , условия, которое совершенно не зависит от фактического вычисления этого числа  $P/(2\lambda)^{\mu-1}$ .

Вычисление степеней числа 2 по модулю 37 дает 1, 2, 4, 8, 16, 32, 27, . . . , 14, 28, 19, 1, 2, 4, . . . . Так как эта последовательность до начала повторения содержит полностью 36 членов, то число 2 есть примитивный корень по модулю 37. Значит, по определению, целое число  $P$  получается подстановкой в полином

$$\varphi(x) = 1 + 2x + 4x^2 + 8x^3 + 16x^4 + 32x^5 + 27x^6 + 17x^7 + \dots \\ \dots + 14x^{33} + 28x^{34} + 19x^{35}$$

примитивного корня  $\beta$  36-й степени из единицы и вычисления произведения  $P = \varphi(\beta) \varphi(\beta^3) \varphi(\beta^5) \dots \varphi(\beta^{33}) \varphi(\beta^{35})$ . Тогда, как показано в предыдущем параграфе,

$$h = \pm \frac{P}{(2 \cdot 37)^{17}} \cdot h_2.$$

В настоящем же параграфе нам предстоит показать, что целое число  $h$  делится на 37.

Не совсем очевидно даже то, что число  $P = \varphi(\beta) \varphi(\beta^3) \dots \dots \varphi(\beta^{35})$  является *целым*, а уж тем более что оно делится на  $2^{17} \cdot 37^{17}$ , как это должно быть для того, чтобы первый сомножитель был (как утверждал Куммер) целым числом. Доказательство того, что  $P$  — целое число, сразу получается из такого общего факта: если  $f(\beta) = a_0 + a_1\beta + a_2\beta^2 + \dots + a_n\beta^n$  — число, представленное в виде полинома от примитивного корня  $\beta$   $k$ -й степени из единицы, и если  $f(\beta)$  при подстановке вместо  $\beta$  любого другого примитивного корня  $\beta'$   $k$ -й степени из единицы дает то же самое число  $f(\beta) = f(\beta')$ , то число  $f(\beta)$  обязательно целое. [На языке теории Галуа: любой целый элемент кругового поля  $k$ -й степени, инвариантный относительно группы Галуа, есть целое рациональное число.] В случае  $k = 36$  примитивный корень  $\beta'$  должен быть нечетной степенью корня  $\beta$ , поэтому легко видеть, что подстановка  $\beta \mapsto \beta'$  лишь переставляет нечетные степени корня  $\beta$ , а значит, оставляет  $P$  без изменения. Таким образом, тот факт, что  $P$  — целое число, непосредственно следует из этой теоремы. По поводу доказательства самой теоремы см. упр. 1.

Главным шагом в доказательстве делимости числа  $P$  на  $37^{17}$  является применение алгебраического тождества, которое полу-

чится, если заметить, что  $\varphi(x)$ , по определению, совпадает с полиномом  $1 + 2x + (2x)^2 + (2x)^3 + \dots + (2x)^{35} = [(2x)^{36} - 1]/(2x - 1)$ , после того как его коэффициенты редуцированы по модулю 37. Поэтому умножим полином  $\varphi(x)$  на  $2x - 1$ :

$$(2x - 1)\varphi(x) = 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + 0 \cdot x^4 + 0 \cdot x^5 + \\ + 37 \cdot x^6 + 37 \cdot x^7 + 0 \cdot x^8 + \dots + 0 \cdot x^{34} + 37 \cdot x^{35} + 38 \cdot x^{36} - 1.$$

Если подставить в это тождество  $x = \beta, \beta^3, \beta^5, \dots, \beta^{35}$  и перемножить все полученные равенства, то найдем, что

$$(2\beta - 1)(2\beta^3 - 1) \dots (2\beta^{35} - 1)P = 37^{18}\psi(\beta)\psi(\beta^3) \dots \psi(\beta^{35}),$$

где  $\psi$  определяется как полином

$$\psi(x) = 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + 0 \cdot x^4 + 0 \cdot x^5 + 1 \cdot x^6 + 1 \cdot x^7 + \\ + 0 \cdot x^8 + \dots + 0 \cdot x^{34} + 1 \cdot x^{35} + 1 \cdot x^{36}.$$

(Заметим, что  $38\beta^{36} - 1 = 37 = 37\beta^{36}$ .) Далее, число  $(2\beta - 1)(2\beta^3 - 1) \dots (2\beta^{35} - 1)$  является целым по той же причине, что и число  $P$ , и это целое число может быть явно найдено посредством формулы

$$(X - \beta)(X - \beta^3) \dots (X - \beta^{35}) = X^{18} + 1$$

(обе части равенства являются полиномами с 18 различными корнями  $\beta, \beta^3, \dots, \beta^{35}$ ), из которой получаем

$$(x - \beta y)(x - \beta^3 y) \dots (x - \beta^{35} y) = x^{18} + y^{18}, \\ (2\beta - 1)(2\beta^3 - 1) \dots (2\beta^{35} - 1) = 1 + 2^{18}.$$

Поскольку 2 — примитивный корень по модулю 37, теорема Ферма дает  $2^{18} \equiv -1 \pmod{37}$  и, значит, 37 должно делить  $2^{18} + 1$ . И на самом деле  $2^{18} + 1 = 262\,145 = 37 \cdot 7085$ . Отсюда

$$7085 \cdot P = 37^{17}\psi(\beta)\psi(\beta^3) \dots \psi(\beta^{35}).$$

Поскольку 37 не делит 7085 и поскольку  $\psi(\beta)\psi(\beta^3) \dots \psi(\beta^{35})$  — целое число, это показывает, что  $P$  делится на  $37^{17}$ .

Сходными рассуждениями можно доказать, что  $P$  делится также на  $2^{17}$ , и тем самым установить, что первый сомножитель  $P/(2 \cdot 37)^{17}$  числа классов в самом деле является целым числом. Однако этот факт нам в дальнейшем не понадобится, и поэтому его доказательство отнесено в упражнения (см. упр. 2).

Вопрос о делимости целого числа  $h$  на 37 совпадает, благодаря равенству в целых числах  $2^{17} \cdot h = \pm (P/37^{17}) \cdot h_2$ , с вопросом о делимости на 37 одного из целых чисел  $P/37^{17}$  или  $h_2$ . Чтобы доказать, что  $h$  делится на 37, достаточно доказать, что  $P/37^{17}$  делится на 37, а для этого достаточно доказать, что

$$\psi(\beta)\psi(\beta^3) \dots \psi(\beta^{35}) \equiv 0 \pmod{37},$$

поскольку отсюда вытекает, что  $7085P$  делится на  $37^{18}$ . Теперь заметим, что при подсчетах по модулю 37 число 2 обладает теми же свойствами, что и число  $\beta$ , а именно,  $2^{36} \equiv 1 \pmod{37}$ , но  $2^j \not\equiv 1 \pmod{37}$  при  $0 < j < 36$ . Значит, мы можем считать, что

$$\psi(\beta) \psi(\beta^3) \dots \psi(\beta^{35}) \equiv \psi(2) \psi(2^3) \dots \psi(2^{35}) \pmod{37},$$

поскольку все упрощения <sup>1)</sup>, использованные для исключения  $\beta$  из выражения целого числа в левой части сравнения, можно применить к числу 2 по модулю 37 в правой части. Следовательно, для того чтобы доказать, что 37 делит первый сомножитель своего числа классов, достаточно доказать, что одно из целых чисел  $\psi(2)$ ,  $\psi(2^3)$ ,  $\psi(2^5)$ , ...,  $\psi(2^{35})$  есть нуль по модулю 37.

Поскольку степени числа 2 по модулю 37 и значения полинома  $\psi(x)$  можно без труда выписать в явном виде, легко вычислить эти 18 целых чисел по модулю 37. Выполнив это, мы найдем, что  $\psi(2^{31}) \equiv 0 \pmod{37}$ , а это и доказывает иррегулярность числа 37. Однако Куммер сумел упростить задачу еще дальше и избежать даже этого простого вычисления следующим образом. Пусть  $b_1, b_2, \dots, b_{36}$  представляют собой коэффициенты полинома  $\psi(x) = b_1x + b_2x^2 + \dots + b_{36}x^{36}$ , и пусть  $\gamma_0, \gamma_1, \dots, \gamma_{35}$  — коэффициенты полинома  $\varphi(x) = \gamma_0 + \gamma_1x + \gamma_2x^2 + \dots + \gamma_{35}x^{35}$ , так что, по определению,  $0 < \gamma_j < 37$ ,  $\gamma_j \equiv 2^j \pmod{37}$ ,  $(2x - 1)\varphi(x) = 37 \cdot \psi(x) + (x^{36} - 1)$  и, следовательно,  $2\gamma_{j-1} - \gamma_j = 37b_j$  при  $j = 1, 2, \dots, 35$  и  $2\gamma_{35} - 1 = 37b_{36}$ . Тогда

$$\begin{aligned} \psi(2^n) &= b_12^n + b_22^{2n} + \dots + b_{36}2^{36n} \equiv \\ &\equiv b_1\gamma_1^n + b_2\gamma_2^n + \dots + b_{36}\gamma_{36}^n \pmod{37}. \end{aligned}$$

Но ясно, что все  $b_j$  равны 0 или 1, а точнее,  $b_j$  равно 0, если  $2\gamma_{j-1} < 37$ , и 1, если  $2\gamma_{j-1} > 37$ . (Это выполняется и при  $j = 36$ .) Значит,  $\psi(2^n) = \sum \gamma_j^n$ , где  $j$  пробегает все индексы, для которых  $\gamma_{j-1} \geq 19$ . Здесь можно сделать упрощение, заметив, что  $\gamma_j^n \equiv (2\gamma_{j-1})^n \equiv \gamma_n \gamma_{j-1}^n$ , откуда

$$\begin{aligned} \psi(2^n) &\equiv \gamma_n [b_1\gamma_0^n + b_2\gamma_1^n + \dots + b_{36}\gamma_{35}^n] \pmod{37} \\ &= \gamma_n [19^n + 20^n + \dots + 36^n], \end{aligned}$$

поскольку каждое целое  $m$  от 1 до 36 точно один раз встречается как некоторое  $\gamma_j$ , а соответствующее  $b_{j+1}$  равно 1 тогда и только тогда, когда  $m \geq 19$ . Значит, для того чтобы определить, делится ли  $\psi(2^n)$  на 37, необходимо и достаточно определить, делится ли  $19^n + 20^n + \dots + 36^n$  на 37.

<sup>1)</sup> Данное сравнение лучше рассматривать как сравнение по модулю общего простого дивизора чисел  $\beta - 2$  и 37. Однако для его установления требуется теория дивизоров для чисел, построенных из корня  $\beta$  36-й степени из единицы, но эта теория не изучалась в гл. 4, поскольку число 36, разумеется, не простое.

Формула для суммы последовательных  $n$ -х степеней была выведена Якобом Бернулли в XVIII в. В современных обозначениях эту формулу можно вкратце описать следующим образом. При любом  $n = 0, 1, 2, \dots$  обозначим через  $B_n(x)$  полином, для которого

$$\int_x^{x+1} B_n(t) dt = x^n.$$

Легко видеть, что это тождество определяет единственный полином  $n$ -й степени (упр. 3). Тогда ясно, что

$$\begin{aligned} M^n + (M+1)^n + \dots + N^n &= \int_M^{M+1} B_n(t) dt + \\ &+ \int_{M+1}^{M+2} B_n(t) dt + \dots + \int_N^{N+1} B_n(t) dt = \int_M^{N+1} B_n(t) dt, \end{aligned}$$

и нахождение формулы для суммы последовательных  $n$ -х степеней, по существу, сводится к нахождению формулы для  $B_n(x)$ . Далее, дифференцирование определяющего уравнения по пределам интегрирования дает

$$\begin{aligned} B_n(x+1) - B_n(x) &= nx^{n-1}, \\ \int_x^{x+1} \frac{d}{dt} B_n(t) dt &= n \int_x^{x+1} B_{n-1}(t) dt, \end{aligned}$$

откуда следует, что  $dB_n(t)/dt = nB_{n-1}(t)$ . Значит, для того чтобы найти полином  $B_n(t)$ , достаточно знать  $B_{n-1}(t)$  и  $B_n(0)$ . В явном виде, обозначив через  $B_n$  постоянную  $B_n(0)$ , получаем

$$B_0(x) = 1 = B_0,$$

$$B_1(x) = \int B_0(x) dx + \text{const} = x + B_1,$$

$$B_2(x) = \int 2B_1(x) dx + \text{const} = x^2 + 2B_1x + B_2,$$

$$B_3(x) = \int 3B_2(x) dx + \text{const} = x^3 + 3B_1x^2 + 3B_2x + B_3,$$

$$B_4(x) = x^4 + 4B_1x^3 + 6B_2x^2 + 4B_3x + B_4$$

и, вообще,

$$\begin{aligned} B_n(x) &= x^n + nB_1x^{n-1} + \\ &+ \frac{n(n-1)}{2} B_2x^{n-2} + \dots + \binom{n}{k} B_kx^{n-k} + \dots + B_n, \end{aligned}$$

где через  $\binom{n}{k}$  обозначен биномиальный коэффициент  $n!/(n-k)!k!$ . Следовательно, вопрос заключается в нахождении так называемых чисел Бернулли  $B_0, B_1, B_2, \dots$ . Нахождение этих чисел облегчается, если заметить, что при  $n \geq 1$

$$0^n = \int_0^1 B_n(t) dt = \frac{B_{n+1}(1) - B_{n+1}(0)}{n+1} \quad (n \geq 1),$$

откуда вытекает, что при  $n \geq 1$

$$B_{n+1}(1) = B_{n+1}(0),$$

$$B_0 + (n+1)B_1 + \dots + \binom{n+1}{k}B_k + \dots + (n+1)B_n + B_{n+1} = B_{n+1},$$

$$B_n = -\frac{1}{n+1} \left[ B_0 + (n+1)B_1 + \dots + \frac{n(n+1)}{2}B_{n-1} \right].$$

Таким образом <sup>1)</sup>,

$$B_1 = -\frac{1}{2}[1] = -\frac{1}{2},$$

$$B_2 = -\frac{1}{3} \left[ 1 + 3 \left( -\frac{1}{2} \right) \right] = \frac{1}{6},$$

$$B_3 = -\frac{1}{4} \left[ 1 + 4 \left( -\frac{1}{2} \right) + 6 \left( \frac{1}{6} \right) \right] = 0,$$

$$B_4 = -\frac{1}{5} \left[ 1 + 5 \left( -\frac{1}{2} \right) + 10 \left( \frac{1}{6} \right) + 10 \cdot 0 \right] = -\frac{1}{30},$$

$$B_5 = -\frac{1}{6} \left[ 1 + 6 \left( -\frac{1}{2} \right) + 15 \left( \frac{1}{6} \right) + 20 \cdot 0 + 15 \left( -\frac{1}{30} \right) \right] = 0,$$

и т. д. Эйлер вычислил значения  $B_n$  для  $n \leq 30$ . Для нечетных  $n$ , больших 1,  $B_n = 0$  (упр. 5). Для четных  $n$  числа  $B_n$  имеют чередующиеся знаки (упр. 6) и очень быстро растут по абсолютной величине при  $n \rightarrow \infty$ . Например, последнее из вычисленных Эйлером чисел равно

$$B_{30} = \frac{8\,615\,841\,276\,005}{14\,322}.$$

В 1842 г. М. Ом опубликовал в известном журнале Крелля [О1] значения всех чисел Бернулли до  $B_{62}$  включительно, так что эти значения наверняка были в распоряжении Куммера в 1847 г.

Итак, рассматриваемые нами суммы равны

$$19^n + 20^n + \dots + 36^n = \int_{19}^{37} B_n(t) dt = \frac{B_{n+1}(37) - B_{n+1}(19)}{n+1},$$

<sup>1)</sup> Из этой формулы легко следует описание чисел Бернулли через разложение функции  $x/(e^x - 1)$ , которое было упомянуто в § 6.1.



где, разумеется,  $B_{n+1}(37)$  и  $B_{n+1}(19)$  — значения полиномов Бернулли, а не произведения чисел Бернулли на 37 и 19. Так как все числа  $n + 1 = 2, 4, \dots, 36$  обратимы по модулю 37, то вопрос о том, делится ли эта сумма на 37, совпадает с вопросом о том, верно ли сравнение  $B_{n+1}(37) - B_{n+1}(19) \equiv 0 \pmod{37}$ . Хотелось бы сказать, что в силу сравнения  $37 \equiv 0 \pmod{37}$  все слагаемые в  $B_{n+1}(37)$ , кроме свободного члена, можно отбросить. Однако полином  $B_{n+1}(x)$  имеет *рациональные* коэффициенты, а не целые, и поэтому обращаться с ним нужно с особой осторожностью.

Оказывается, число  $B_{n+1}(37) - B_{n+1}(19)$  является целым, несмотря на то что некоторые члены полинома  $B_{n+1}(x)$  нецелые и даже несмотря на то что каждое из чисел  $B_{n+1}(37)$  и  $B_{n+1}(19)$  не является целым (см. упр. 7). Вычисление этого целого числа требует вдобавок к сложению, вычитанию и умножению еще и *деления*, а именно деления на знаменатели чисел Бернулли, встречающихся в качестве коэффициентов в  $B_{n+1}(x)$ , но все дело в том, что в итоге получается рациональное число, знаменатель которого равен 1. Однако, как явствует из приведенной выше формулы для чисел Бернулли, при  $n < 35$  в вычислениях никогда не потребуются деление на число, кратное 37; лишь в случае  $B_{36}$  приходится делить на 37, но  $B_{36}$  входит в  $B_{36}(x)$  в качестве свободного члена и уничтожается в разности  $B_{36}(37) - B_{36}(19)$ . Следовательно, так как деление на любое целое число, не кратное 37, по модулю 37 *допустимо*, то можно выполнить все вычисление по модулю 37, определив тем самым не само целое число  $B_{n+1}(37) - B_{n+1}(19)$ , а только его вычет по модулю 37. Но это и есть все, что нам требуется.

[Эти рассуждения аналогичны предшествующим, когда для вычисления целого числа  $\psi(\beta) \psi(\beta^3) \dots \psi(\beta^{35})$  по модулю 37 мы брали число 2 вместо  $\beta$ , пользуясь тем, что 2 — примитивный корень 36-й степени из единицы по модулю 37. Подобным же образом, дальше мы будем вычислять  $B_{n+1}(19) - B_{n+1}$ , полагая  $19 \equiv \equiv 1/2 \pmod{37}$ . Хотя вначале это выглядит очень странно, в действительности совершенно естественно придать именно такой *смысл* числу  $1/2$ , поскольку оно является тем числом  $x$ , для которого  $2x = 1$ , а по модулю 37 это как раз 19.]

Итак, числа Бернулли можно найти по модулю 37 (за исключением последнего  $B_{36}$ ), и сравнение  $B_{n+1}(37) - B_{n+1}(19) \equiv \equiv 0 \pmod{37}$  становится вполне осмысленным. Поскольку, конечно,  $37 \equiv 0 \pmod{37}$ , мы непосредственно видим, что все члены в  $B_{n+1}(37)$ , кроме свободного члена, равны нулю, и остается определить, является ли  $B_{n+1} - B_{n+1}(19)$  нулем по модулю 37. Куммер достиг этого при помощи остроумного приема: он заметил, что  $19 \equiv 1/2 \pmod{37}$ , и воспользовался специальной формулой для  $B_n(1/2)$ .

Нужное тождество может быть выведено следующим образом <sup>1)</sup>. Из определяющего равенства вытекает, что

$$2^m x^m = \int_{2x}^{2x+1} B_m(t) dt = 2 \int_x^{x+1/2} B_m(2u) du;$$

с другой стороны,

$$2^m x^m = 2^m \int_x^{x+1} B_m(t) dt = 2^m \int_x^{x+1/2} \left[ B_m(t) + B_m\left(t + \frac{1}{2}\right) \right] dt.$$

Отсюда следует, что

$$2^m \left[ B_m(x) + B_m\left(x + \frac{1}{2}\right) \right] = 2B_m(2x)$$

(ибо эти два полинома имеют одинаковые интегралы по всем интервалам длины  $1/2$ ). Таким образом, при  $x=0$  и  $m=n+1$  получаем

$$B_{n+1} + B_{n+1}(1/2) = 2^{-n} B_{n+1},$$

$$B_{n+1}(1/2) - B_{n+1} = (2^{-n} - 2) B_{n+1} = (1/2)^n (1 - 2^{n+1}) B_{n+1}.$$

Это равенство рациональных чисел можно истолковать так: действия сложения, вычитания, умножения и деления, требуемые для нахождения  $B_{n+1}(1/2) - B_{n+1}$ , приводят к тому же результату, что и эти же действия, требуемые для  $(1/2)^n (1 - 2^{n+1}) B_{n+1}$ . (Оба выражения можно привести к виду  $\pm p/q$ , т. е. их можно упрощать до тех пор, пока будет требоваться лишь одно умножение на целое число и одно деление на положительное целое число.) То же самое верно, если рассматривать эти действия как действия над целыми числами по модулю 37, при условии что не потребуется делить на число, кратное 37. Так как при  $n < 36$  число  $B_n$  не требует деления на 37 и так как деление на 2 по модулю 37 равносильно умножению на 19, то это доказывает, что при  $n = 1, 3, 5, \dots, 33$

$$B_{n+1}(19) - B_{n+1} \equiv 19^n (1 - 2^{n+1}) B_{n+1} \pmod{37},$$

при условии что числа  $B_{n+1}$  рассматриваются как целые числа по модулю 37, получаемые делением (по модулю 37) числителя на знаменатель. Правая часть может быть нулем по модулю 37, только если  $2^{n+1} - 1$  или  $B_{n+1}$  есть нуль по модулю 37, но

<sup>1)</sup> Этот вывод отличается от вывода Куммера. Куммер считал, что это тождество получено им впервые ([K14], стр. 478), и Смит ([S3], стр. 117) повторяет это мнение. Интересно, что эта основная формула исчисления разностей (см. Нёрлунд [N3]) была открыта в ходе исследований по Последней теореме Ферма.

$2^{n+1} \not\equiv 1 \pmod{37}$  при  $n = 1, 3, \dots, 33$ , поэтому мы доказали, что, за исключением случая  $n = 35$ , сравнение  $19^n + 20^n + \dots + 36^n \equiv 0 \pmod{37}$  равносильно утверждению о том, что числитель  $B_{n+1}$  делится на 37. Следовательно, задачу выяснения делимости чисел  $\psi(2^n)$  на 37 при  $n = 1, 3, \dots, 33$  можно решить, попросту обратившись к таблице чисел Бернулли и посмотрев, делятся ли на 37 числители чисел  $B_2, B_4, \dots, B_{34}$ . И вот оказывается, что числитель числа  $B_{32}$ , равный 7 709 321 041 217 по таблице Ома, делится на 37. (Делимость на 37 легко усмотреть, если заметить, что 37 делит 111. Поэтому из того, что числитель  $B_{32}$  равен  $111 \cdot 69\,453\,342\,713 + 74$ , следует его делимость на 37. Этот же прием позволяет выяснить, выполняется ли сравнение  $\psi(2^n) \equiv 0 \pmod{37}$  для других значений  $n = 1, 3, 5, \dots, 33$ . Ответ таков: только  $\psi(2^{31})$  делится на 37.) Таким образом,  $37^{18}$  делит  $P$ , 37 делит  $h = \pm P \cdot 37^{-17} \times \times 2^{-17} \cdot h_2$  и  $\lambda = 37$  не удовлетворяет куммерову условию (A), т. е. 37 есть иррегулярное простое. Этим завершается доказательство, бывшее темой этого параграфа.

## Упражнения

1. Докажите, что если  $\beta$  — примитивный корень  $n$ -й степени из единицы и  $g(\beta) = a_0 + a_1\beta + \dots + a_{n-1}\beta^{n-1}$  — полином от  $\beta$  с целыми коэффициентами, обладающий тем свойством, что  $g(\beta') = g(\beta)$  для всех примитивных корней  $\beta'$   $n$ -й степени из единицы, то  $g(\beta)$  — целое число.

2. Докажите, что  $2^{u-1}$  делит  $P$ . (См. [B2, § 5.5.3].)

3. Покажите, что если  $p(x) = a_N x^N + a_{N-1} x^{N-1} + \dots + a_0$ , то равенство  $\int_x^{x+1} p(t) dt = x^n$  однозначно определяет рациональные числа  $a_N, a_{N-1}, \dots, a_0$  при условии, что  $N \geq n$ .

4. Докажите математической индукцией, что  $B_n(x) = \sum_{k=0}^n \binom{n}{k} B_k x^{n-k}$ .

5. Докажите, что  $B_n(1-t) = (-1)^n B_n(t)$ . [Прямо используйте определяющее уравнение для  $B_n(x)$ .] Установите, что  $B_{2n+1} = 0$  при  $n > 0$ .

6. Исследуйте изменение знака функции  $B_n(t)$  при  $0 \leq t \leq 1$  и, в частности, докажите, что знаки чисел  $B_{2n}$  и  $B_{2n+2}$  противоположны при  $n > 0$ .

7. Докажите, что если  $B_n$  не является целым числом, то  $B_n(x)$  не принимает целых значений при целых  $x$ .

8. Подсчитайте  $\psi(2^n)$  по модулю 37 прямым использованием определения при  $n = 1, 2, \dots, 35$ .

9. Подсчитайте  $B_0, B_1, \dots, B_{10}$  по модулю 13, построив вначале треугольник Паскаля по модулю 13. Вычислите  $B_n(1/2)$  по модулю 13 двумя способами: во-первых, используя  $1/2 \equiv 7 \pmod{13}$ , а во-вторых, используя тождество для  $B_n(1/2)$ .

10. Докажите, что  $\psi(2^{35})$  не делится на 37. [Один способ состоит в прямом подсчете значения  $\psi(2^{35})$  по модулю 37. Второй заключается в применении метода, используемого для общего случая в следующем параграфе. Третий — следующий:  $B_{36}(1/2) - B_{36} = -(1/2)^{36} (2^{18} - 1)(2^{18} + 1) B_{36}$ . Таким образом, для того чтобы показать, что  $B_{36}(19) - B_{36}$  не делится на 37, достаточно

показать, что  $37B_{36}$  есть рациональное число, у которого ни числитель, ни знаменатель не делятся на 37. Куммер называет это «известным свойством» чисел Бернулли. (Это частный случай *теоремы фон Штаудта*.) Так как  $37B_{36} = -[1 + 37B_1 + \binom{37}{2}B_2 + \dots + \binom{37}{35}B_{35}]$ , то ясно, что в числе  $37B_{36}$  отсутствует деление на 73. Разделите 37 ( $1^{36} + 2^{36} + 3^{36} + \dots + 36^{36}$ )  $= B_{37}(37) - B_{37}$  на 37 и, рассматривая это как сравнение по модулю 37, найдите сравнение  $-1 \equiv 37B_{36}$ .]

### 6.16. Делимость первого сомножителя на $\lambda$

Для того чтобы ответить на тот же вопрос, что и в предыдущем параграфе (т. е. «делится ли  $P/\lambda^{\mu-1}$  на  $\lambda$ ?»), в случае произвольного простого  $\lambda$ , по модулю которого число 2 является примитивным корнем, нужна лишь небольшая модификация проведенных там рассуждений. Результат таков: число  $P/\lambda^{\mu-1}$  тогда и только тогда делится на  $\lambda$ , когда числитель одного из чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$  делится на  $\lambda$ . Если 2 не является примитивным корнем по модулю  $\lambda$ , то необходимая модификация менее очевидна, но окончательная теорема остается той же самой.

Рассмотрим, например, случай  $\lambda = 31$ . Здесь число 2 не является примитивным корнем, поскольку  $2^5 \equiv 1 \pmod{31}$ . Однако, как было отмечено в § 4.7, 3 — примитивный корень. При  $\gamma = 3$  находим  $\varphi(x) = 1 + 3x + 9x^2 + 27x^3 + 19x^4 + \dots + 21x^{29}$ . Значит,  $(3x - 1)\varphi(x) = 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + 62 \cdot x^4 + \dots + 63 \cdot x^{30} - 1 = 31(b_1x + b_2x^2 + \dots + b_{30}x^{30}) + (x^{30} - 1)$ , где  $b_j$  определяются условиями  $31b_j = 3\gamma_{j-1} - \gamma_j$ ,  $\gamma_j \equiv 3^j \pmod{31}$ ,  $0 < \gamma_j < 31$ . Определив  $\psi(x)$  этим равенством  $(3x - 1)\varphi(x) = 31\psi(x) + (x^{30} - 1)$ , обозначим через  $\beta$  примитивный корень 30-й степени из единицы и, перемножив 15 равенств, полученных заменой  $x = \beta^j$  при  $j = 1, 3, \dots, 29$ , найдем, по определению  $P$ , что

$$(3^{15} + 1)P = 31^{15}\psi(\beta)\psi(\beta^3)\dots\psi(\beta^{29}).$$

Далее,  $3^{15} + 1$  делится на 31, поскольку  $(3^{15})^2 \equiv 1 \pmod{31}$  (теорема Ферма), но  $3^{15} \not\equiv 1 \pmod{31}$  (3 — примитивный корень). Однако  $3^{15} + 1$  не делится на  $31^2$ , поскольку, как показывает короткий подсчет,  $3^{15} + 1 \equiv 7 \cdot 31 \pmod{31^2}$ . Значит, найденное равенство показывает, что  $P$  делится на  $31^{14}$  и что частное тогда и только тогда делится на 31, когда  $\psi(\beta)\psi(\beta^3)\dots\psi(\beta^{29}) \equiv 0 \pmod{31}$ . Но  $\psi(\beta)\psi(\beta^3)\dots\psi(\beta^{29}) \equiv \psi(3)\psi(3^3)\dots\psi(3^{29}) \pmod{31}$  (ибо по модулю 31 целое число 3 удовлетворяет всем соотношениям, которым удовлетворяет  $\beta$ ), поэтому выяснение того, имеет ли место сравнение  $P/31^{14} \equiv 0 \pmod{31}$ , равносильно выяснению того, является ли нулем по модулю 31 какое-либо из целых чисел  $\psi(3), \psi(3^3), \dots, \psi(3^{29})$ .

Далее, имеем  $\psi(3^n) = b_13^n + b_23^{2n} + \dots + b_{30}3^{30n} \equiv b_1\gamma_1^n + b_2\gamma_2^n + \dots + b_{30}\gamma_{30}^n \equiv b_1(3\gamma_0)^n + \dots + b_{30}(3\gamma_{29})^n \equiv \gamma_n[b_1\gamma_0^n + b_2\gamma_1^n + \dots + b_{30}\gamma_{29}^n]$ , где  $b_j$  определены условием

$31b_j = 3\gamma_{j-1} - \gamma_j$ . Так как  $-31 < -\gamma_j < 31b_j < 3\gamma_{j-1} < 3 \cdot 31$ , то  $-1 < b_j < 3$ , т. е.  $b_j = 0, 1$  или  $2$ . Кроме того, если  $b_j = 0$ , то число  $3\gamma_{j-1} = \gamma_j$  лежит между  $0$  и  $31$ , если  $b_j = 1$ , то число  $3\gamma_{j-1} = \gamma_j + 31$  лежит между  $31$  и  $2 \cdot 31$ , и если  $b_j = 2$ , то число  $3\gamma_{j-1} = \gamma_j + 2 \cdot 31$  лежит между  $2 \cdot 31$  и  $3 \cdot 31$ . Иными словами,  $b_j = 0$  при  $\gamma_{j-1} = 1, 2, \dots, 10$ ;  $b_j = 1$  при  $\gamma_{j-1} = 11, 12, \dots, 20$  и  $b_j = 2$  при  $\gamma_{j-1} = 21, 22, \dots, 30$ . Поскольку каждое целое число от  $1$  до  $30$  встречается точно один раз в качестве  $\gamma_j$ , отсюда следует, что

$$\psi(3^n) \equiv \gamma_n [11^n + 12^n + \dots + 20^n + 2 \cdot 21^n + 2 \cdot 22^n + \dots + 2 \cdot 30^n] \pmod{31}.$$

Так как  $\gamma_n \not\equiv 0 \pmod{31}$ , то вопрос о делимости этого целого числа на  $31$  совпадает с вопросом о делимости на  $31$  целого числа

$$(11^n + 12^n + \dots + 30^n) + (21^n + 22^n + \dots + 30^n) = \\ = \int_{11}^{31} B_n(t) dt + \int_{21}^{31} B_n(t) dt = \frac{B_{n+1}(31) - B_{n+1}(11) + B_{n+1}(31) - B_{n+1}(21)}{n+1}.$$

За исключением случая  $n = 29$ , все числа Бернулли, входящие в это равенство, можно рассматривать как целые числа по модулю  $31$  (т. е. они не требуют деления ни на какое кратное числа  $31$ ), и, поскольку  $B_{n+1}(31) \equiv B_{n+1}(0) = B_{n+1} \pmod{31}$ , отсюда вытекает, что  $\psi(3^n) \equiv 0 \pmod{31}$  тогда и только тогда, когда  $B_{n+1}(11) + B_{n+1}(21) \equiv 2B_{n+1}$  (при  $n = 1, 3, \dots, 27$ , но не при  $n = 29$ ).

Далее, имеем  $3 \cdot 11 \equiv 2 \pmod{31}$  и  $3 \cdot 21 \equiv 1 \pmod{31}$ , так что рассматриваемое сравнение можно переписать в виде  $B_{n+1}(2/3) + B_{n+1}(1/3) \equiv 2B_{n+1}$ . Прием, использованный в предыдущем параграфе при выводе тождества для  $B_n(1/2)$ , непосредственно обобщается, и мы получаем

$$3^m x^m = \int_{3x}^{3x+1} B_m(t) dt = 3 \int_x^{x+1/3} B_m(3u) du, \\ 3^m x^m = 3^m \int_x^{x+1} B_m(t) dt = 3^m \int_x^{x+1/3} [B_m(t) + B_m(t+1/3) + B_m(t+2/3)] dt, \\ 3^{1-m} B_m(3x) = B_m(x) + B_m(x+1/3) + B_m(x+2/3), \\ B_{n+1} + B_{n+1}(1/3) + B_{n+1}(2/3) = 3^{-n} B_{n+1}.$$

Рассматриваемое сравнение принимает вид

$$3^{-n} B_{n+1} \equiv 3B_{n+1}, \\ (1/3)^n (3^{n+1} - 1) B_{n+1} \equiv 0 \pmod{31},$$

а это сравнение при  $n = 1, 3, \dots, 27$  верно в тех и только тех случаях, когда числитель числа  $B_{n+1}$  делится на 31. По таблице чисел Бернулли можно проверить, что это не выполняется ни для какого из случаев  $n = 1, 3, 5, \dots, 27$ , т. е.  $\psi(3^n) \not\equiv 0$  при  $n = 1, 3, \dots, 27$ .

Обратимся к случаю  $n = 29$ . В этом случае можно прямо доказать, что  $\psi(3^{29}) \not\equiv 0 \pmod{31}$ . Это делается так. Пусть  $3^{30} - 1 = (3^{15} - 1)(3^{15} + 1) = 31\nu$ , где, как уже отмечалось,  $\nu$  не делится на 31. Тогда определяющее полином  $\psi$  равенство, а именно  $(3x - 1)\varphi(x) = 31\psi(x) + (x^{30} - 1)$ , при  $x = 3^{29}$  дает  $(3^{30} - 1)\varphi(3^{29}) = 31\psi(3^{29}) + (3^{30})^{29} - 1$ ,  $\nu\varphi(3^{29}) = \psi(3^{29}) + [(1 + 31\nu)^{29} - 1] \cdot 31^{-1}$ . По определению полинома  $\varphi$  мы непосредственно видим, что  $\varphi(3^{29}) \equiv 1 + 3^{30} + 3^{60} + \dots \equiv 1 + 1 + \dots + 1 = 30 \equiv -1 \pmod{31}$ . Следовательно,  $\psi(3^{29}) = \nu\varphi(3^{29}) - 29\nu - \binom{29}{2}\nu^2 31 - \dots \equiv -\nu - 29\nu \equiv \nu \not\equiv 0 \pmod{31}$ , что и требовалось показать.

Для выяснения делимости  $P$  на степени  $\lambda$  в общем случае можно использовать сходную технику. Пусть  $\lambda$  — нечетное простое число и  $\gamma$  — примитивный корень по модулю  $\lambda$ . Пусть  $\varphi(x) = 1 + \gamma_1 x + \gamma_2 x^2 + \dots + \gamma_{\lambda-2} x^{\lambda-2}$ , где  $\gamma_j$  определяется условиями  $\gamma_j \equiv \gamma^j \pmod{\lambda}$ ,  $0 < \gamma_j < \lambda$ . Тогда, по определению,  $P = \varphi(\beta)\varphi(\beta^3)\dots\varphi(\beta^{\lambda-2})$ , где  $\beta$  — примитивный корень  $(\lambda - 1)$ -й степени из единицы. Определим  $\psi(x)$  равенством  $(\gamma x - 1)\varphi(x) = \lambda\psi(x) + (x^{\lambda-1} - 1)$ , где  $\psi(x) = b_1 x + b_2 x^2 + \dots + b_{\lambda-1} x^{\lambda-1}$ ,  $\lambda b_j = \gamma\gamma_{j-1} - \gamma_j$ . Тогда перемножение равенств  $(\gamma\beta^j - 1)\varphi(\beta^j) = \lambda\psi(\beta^j)$  при  $j = 1, 3, \dots, \lambda - 2$  дает

$$(\gamma^\mu + 1)P = \lambda^\mu \psi(\beta)\psi(\beta^3)\dots\psi(\beta^{\lambda-2}).$$

Предположим на время, что  $\gamma$  выбрано таким образом, что число  $\gamma^\mu + 1$  (которое обязательно делится на  $\lambda$ ) не делится на  $\lambda^2$ . Тогда это равенство показывает, что  $P$  делится на  $\lambda^{\mu-1}$ , а частное  $P/\lambda^{\mu-1}$  в том и только том случае делится на  $\lambda$ , когда целое число  $\psi(\beta)\psi(\beta^3)\dots\psi(\beta^{\lambda-2})$  делится на  $\lambda$ . Это целое число по модулю  $\lambda$  совпадает с целым числом  $\psi(\gamma)\psi(\gamma^3)\dots\psi(\gamma^{\lambda-2})$  (ибо целое число  $\gamma$  по модулю  $\lambda$  удовлетворяет всем соотношениям, которым удовлетворяет комплексное число  $\beta$ ), и это целое число тогда и только тогда является нулем по модулю  $\lambda$ , когда таков один из сомножителей  $\psi(\gamma), \psi(\gamma^3), \dots, \psi(\gamma^{\lambda-2})$ . Значит, частное  $P/\lambda^{\mu-1}$  тогда и только тогда делится на  $\lambda$ , когда  $\psi_k(\gamma)$ , или  $\psi(\gamma^3), \dots$ , или  $\psi(\gamma^{\lambda-2})$  делится на  $\lambda$  (все еще при условии, что  $\gamma^\mu + 1 \not\equiv 0 \pmod{\lambda^2}$ ).

Так как число  $\lambda b_j = \gamma\gamma_{j-1} - \gamma_j$  лежит между  $-\lambda$  и  $\gamma\lambda$ , то  $b_j$  лежит между  $-1$  и  $\gamma$ , т. е.  $b_j = 0, 1, \dots, \gamma - 1$ . К тому же  $b_j = k$  тогда и только тогда, когда число  $\gamma\gamma_{j-1} = \lambda k + \gamma_j$  лежит между  $k\lambda$  и  $k\lambda + \lambda$ , т. е.  $\gamma_{j-1}$  лежит между  $k(\lambda/\gamma)$  и  $k(\lambda/\gamma) +$



$+(\lambda/\gamma)$ . Так как

$$\begin{aligned}\psi(\gamma^n) &\equiv b_1\gamma_1^n + b_2\gamma_2^n + \dots + b_{\lambda-1}\gamma_{\lambda-1}^n \equiv \\ &\equiv \gamma_n [b_1\gamma_0^n + b_2\gamma_1^n + \dots + b_{\lambda-1}\gamma_{\lambda-2}^n],\end{aligned}$$

а каждое целое число между 0 и  $\lambda$  совпадает с  $\gamma_j$  точно для одного значения  $j$ , то отсюда следует, что число  $\psi(\gamma^n)$  сравнимо по модулю  $\lambda$  с целым числом  $\gamma_n$ , умноженным на

$$\begin{aligned}0 \cdot 1^n + \dots + 0 \cdot (t_1 - 1)^n + 1 \cdot t_1^n + \dots + 1 \cdot (t_2 - 1)^n + 2 \cdot t_2^n + \dots \\ \dots + (\gamma - 2)(t_{\gamma-1} - 1)^n + (\gamma - 1)t_{\gamma-1}^n + \dots + (\gamma - 1)(\lambda - 1)^n = \\ = t_1^n + (t_1 + 1)^n + \dots + (\lambda - 1)^n + t_2^n + (t_2 + 1)^n + \dots \\ \dots + (\lambda - 1)^n + \dots + t_{\gamma-1}^n + (t_{\gamma-1} + 1)^n + \dots + (\lambda - 1)^n,\end{aligned}$$

где через  $t_k$  обозначается наименьшее целое число, большее чем  $k(\lambda/\gamma)$ . Значит,

$$\begin{aligned}\psi(\gamma^n) &\equiv \frac{\gamma_n}{n+1} [B_{n+1}(\lambda) - B_{n+1}(t_1) + B_{n+1}(\lambda) - B_{n+1}(t_2) + \dots \\ &\dots + B_{n+1}(\lambda) - B_{n+1}(t_{\gamma-1})].\end{aligned}$$

За исключением случая  $n = \lambda - 2$ , все числа Бернулли в этом сравнении не требуют деления на кратные числа  $\lambda$ , и поэтому в каждом конкретном случае их можно рассматривать как целые по модулю  $\lambda$ . Целые числа  $t_1, t_2, \dots, t_{\gamma-1}$  сравнимы с  $(1/\gamma), (2/\gamma), \dots, ((\gamma - 1)/\gamma)$  по модулю  $\lambda$  (быть может, в другом порядке) по следующей причине. Для каждого целого  $r$  из интервала  $0 < r < \gamma$  имеется такое целое  $t$  из интервала  $0 < t < \lambda$ , что  $t\gamma \equiv r \pmod{\lambda}$  ( $\gamma$  обратимо по модулю  $\lambda$ ). Таким образом,  $t\gamma - r = k\lambda$  для некоторого  $k$ , большего чем 0 и меньшего чем  $\gamma$  (ибо  $t\gamma - r > 0$  и  $t\gamma - r < t\gamma < \lambda\gamma$ ). Значит, число  $t = k(\lambda/\gamma) + (r/\gamma)$  является наименьшим целым числом, большим чем  $k(\lambda/\gamma)$ , т. е.  $t = t_k$  и  $t_k \equiv r/\gamma \pmod{\lambda}$ . Далее,

$$B_{n+1} + B_{n+1}\left(\frac{1}{\gamma}\right) + B_{n+1}\left(\frac{2}{\gamma}\right) + \dots + B_{n+1}\left(\frac{\gamma-1}{\gamma}\right) = \gamma^{-n}B_{n+1}.$$

Значит, исключая случай  $n = \lambda - 2$ , имеем

$$\begin{aligned}\psi(\gamma^n) &\equiv \frac{\gamma_n}{n+1} \left[ (\gamma - 1)B_{n+1} - B_{n+1}\left(\frac{1}{\gamma}\right) - \right. \\ &\quad \left. - B_{n+1}\left(\frac{2}{\gamma}\right) - \dots - B_{n+1}\left(\frac{\gamma-1}{\gamma}\right) \right] \equiv \\ &\equiv \frac{\gamma_n}{n+1} [\gamma B_{n+1} - \gamma^{-n}B_{n+1}] \equiv \frac{1}{n+1} (\gamma^{n+1} - 1) B_{n+1} \pmod{\lambda}.\end{aligned}$$

Так как  $\gamma^{n+1} - 1 \not\equiv 0 \pmod{\lambda}$  (снова за исключением  $n = \lambda - 2$ ), то это показывает, что  $\psi(\gamma^n) \equiv 0 \pmod{\lambda}$  в том и только том слу-

чае, когда  $B_{n+1} \equiv 0 \pmod{\lambda}$ , т. е. тогда и только тогда, когда числитель числа Бернулли  $B_{n+1}$  делится на  $\lambda$ .

В случае  $n = \lambda - 2$  число  $\psi(\gamma^n)$  не является нулем по модулю  $\lambda$ . Это можно доказать точно так же, как в случае  $\gamma = 3$ ,  $\lambda = 31$ . Определяя  $v$  равенством  $\gamma^{\lambda-1} - 1 = \lambda v$ , полагая  $x = \gamma^{\lambda-2}$  в равенстве  $(\gamma x - 1) \varphi(x) = \lambda \psi(x) + x^{\lambda-1} - 1$ , деля его на  $\lambda$  и редуцируя по модулю  $\lambda$ , мы получаем  $v \varphi(\gamma^{\lambda-2}) \equiv \psi(\gamma^{\lambda-2}) + (\lambda - 2)v \pmod{\lambda}$ . Из сравнения  $\varphi(\gamma^{\lambda-2}) \equiv -1 \pmod{\lambda}$  следует, что  $\psi(\gamma^{\lambda-2}) \equiv v \pmod{\lambda}$ . Так как число  $\gamma^{\lambda-1} - 1 \equiv (\gamma^\mu - 1) \times (\gamma^\mu + 1)$ , по определению корня  $\gamma$ , не делится на  $\lambda^2$ , то  $v \not\equiv 0 \pmod{\lambda}$  и  $\psi(\gamma^{\lambda-2}) \not\equiv 0 \pmod{\lambda}$ , что и требовалось доказать.

Итак, при условии, что имеется такой примитивный корень  $\gamma$  по модулю  $\lambda$ , для которого  $\gamma^\mu + 1 \not\equiv 0 \pmod{\lambda^2}$ , мы полностью доказали следующую теорему.

**Теорема.** Число  $P$  делится на  $\lambda^{\mu-1}$ . Частное тогда и только тогда делится на  $\lambda$ , когда числитель одного из чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$  делится на  $\lambda$ .

Наконец, рассмотрим задачу нахождения примитивного корня  $\gamma$  по модулю  $\lambda$ , для которого  $\gamma^\mu + 1 \not\equiv 0 \pmod{\lambda^2}$ . Пусть  $\gamma$  — любой примитивный корень в интервале  $0 < \gamma < \lambda$ . Если  $\gamma^\mu + 1 \equiv 0 \pmod{\lambda^2}$ , то  $(\gamma + \lambda)^\mu + 1 \equiv \gamma^\mu + \mu \gamma^{\mu-1} \lambda + 1 \equiv \mu \gamma^{\mu-1} \lambda \not\equiv 0 \pmod{\lambda^2}$  и  $\gamma + \lambda$  является примитивным корнем нужного для доказательства типа. Правда, в этом доказательстве молчаливо предполагалось, что  $\gamma$  лежит в интервале  $0 < \gamma < \lambda$  (естественное предположение для целых чисел по модулю  $\lambda$ ). Однако тщательный анализ доказательства показал бы, что требуется лишь предположение  $\gamma > 0$ , при условии <sup>1)</sup> что числа  $t_j$  считаются с соответствующими кратностями. По-другому, можно сохранить предположение  $0 < \gamma < \lambda$  и воспользоваться равенством  $[(\gamma + \lambda)x - 1] \varphi(x) = \lambda \psi(x) + \lambda x \varphi(x) + x^{\lambda-1} - 1$  при  $x = \beta, \beta^3, \dots, \beta^{\lambda-2}$  для нахождения равенства

$$[(\gamma + \lambda)^\mu + 1] P = \lambda^\mu \prod_n [\psi(\beta^n) + \beta^n \varphi(\beta^n)],$$

где в произведении справа индекс  $n$  пробегает значения  $1, 3, \dots, \lambda - 2$ . В рассматриваемом случае  $\gamma^\mu + 1 \equiv 0 \pmod{\lambda^2}$  это показывает, что  $P$  делится на  $\lambda^{\mu-1}$ , а частное тогда и только тогда делится на  $\lambda$ , когда одно из целых чисел  $\psi(\gamma^n) + \gamma^n \varphi(\gamma^n)$  по модулю  $\lambda$  равно 0. За исключением случая  $n = \lambda - 2$ , равенство  $(\gamma^{n+1} - 1) \varphi(\gamma^n) = \lambda \psi(\gamma^n) + \gamma^{(\lambda-1)n} - 1$  показывает, что  $\varphi(\gamma^n) \equiv 0 \pmod{\lambda}$  и  $\psi(\gamma^n) + \gamma^n \varphi(\gamma^n) \equiv \psi(\gamma^n) \equiv (n+1)^{-1} \times (\gamma^{n+1} - 1) B_{n+1} \pmod{\lambda}$ . Следовательно, признаком делимости, как и раньше, является делимость числителя числа  $B_{n+1}$ . В случае  $n = \lambda - 2$  предыдущие рассуждения дают  $\psi(\gamma^{\lambda-2}) \equiv$

<sup>1)</sup> Кажется, Куммер в этом месте проявил некоторую небрежность.

$\equiv v \pmod{\lambda}$ , где  $v$  определяется формулой  $\gamma^{\lambda-1} - 1 = \lambda v$  и, значит,  $v \equiv 0 \pmod{\lambda}$ . Следовательно,  $\psi(\gamma^{\lambda-2}) + \gamma^{\lambda-2}\varphi(\gamma^{\lambda-2}) \equiv \gamma^{\lambda-2}\varphi(\gamma^{\lambda-2}) \equiv \gamma^{-1} \cdot (-1) \not\equiv 0 \pmod{\lambda}$ , и теорема доказана.

## Упражнения

1. Докажите, что  $\psi(\gamma^n) \equiv 0 \pmod{\lambda}$  при  $n = 2, 4, \dots, \lambda - 3$ .
2. Вычислите  $\psi(\gamma^n)$  по модулю  $\lambda$  во всех случаях при  $\lambda \leq 13$  ( $\lambda$  — простое число) и  $0 < n < \lambda$ .

## 6.17. Делимость второго сомножителя на $\lambda$

Куммерово условие (A) состоит в том, что  $h$  не делится на  $\lambda$ . Равенство  $2^{\mu-1}h = (P/\lambda^{\mu-1}) \cdot h_2$  показывает, что это верно тогда и только тогда, когда ни  $P/\lambda^{\mu-1}$ , ни  $h_2$  не делится на  $\lambda$ . Простой признак делимости числа  $P/\lambda^{\mu-1}$  на  $\lambda$  был найден в предыдущем параграфе. Для того чтобы иметь возможность проверять условие (A), нужно также установить критерий делимости  $h_2$  на  $\lambda$ . Куммер обнаружил, что, к счастью, это можно сделать, не зная самого  $h_2$ , поскольку вычисление  $h_2$  во всех случаях крайне трудно. Он показал, что из  $\lambda \mid h_2$  вытекает  $\lambda \mid (P/\lambda^{\mu-1})$ . Значит, если  $\lambda$  не делит  $P/\lambda^{\mu-1}$ , то  $\lambda$  также не делит и  $h_2$ , и условие (A) выполняется.

**Теорема.** Простое число  $\lambda > 2$  удовлетворяет куммерову условию (A) тогда и только тогда, когда оно не делит числители чисел  $B_2, B_4, \dots, B_{\lambda-3}$ .

Итак, для доказательства этой теоремы нужно показать, что из условия  $\lambda \mid h_2$  вытекает критерий с числами Бернулли, или, что равносильно, из этого условия следует  $\lambda \mid (P/\lambda^{\mu-1})$ .

Если  $\lambda \mid h_2$ , то имеется единица, не представимая в виде  $\pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$ , которая после возведения в  $\lambda$ -ю степень дает единицу уже такого вида. В терминах теории групп это следует из того факта, что абелева группа, порядок которой делится на  $\lambda$ , содержит элемент порядка  $\lambda$  (здесь это группа всех единиц по модулю тех из них, которые имеют специальный вид  $\pm \alpha^k \prod (1 - \sigma^h\alpha)^{x_h}$ ). Иначе это можно было бы доказать, исследуя определитель замены координат, вызываемой преобразованием решетки  $\Phi$ -образов единиц специального вида в решетку  $\Phi$ -образов всех единиц (см. упр. 3).

Пусть выбрана такая единица, скажем  $e_0(\alpha)$ , и пусть  $e(\alpha)$  — ее  $\lambda$ -я степень. Тогда  $e(\alpha)$  может быть записана в специальном виде:  $e(\alpha) = \pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$ , где  $x_1 + x_2 + \dots + x_\mu = 0$ . Числа  $x_i$  не все делятся на  $\lambda$ , поскольку, если бы это было не так, то единица  $e(\alpha)$  имела бы вид  $e(\alpha) = \pm \alpha^k e_1(\alpha)^\lambda$ , где  $e_1(\alpha)$  — единица специального вида  $e_1(\alpha) =$

$= (1 - \sigma\alpha)^{y_1} (1 - \sigma^2\alpha)^{y_2} \dots (1 - \sigma^\mu\alpha)^{y_\mu}$ ; тогда частное  $e_0(\alpha) e_1(\alpha)^{-1}$  было бы единицей, которая в  $\lambda$ -й степени равнялась бы  $\pm\alpha^k$ , откуда бы следовало (упр. 2), что  $e_0(\alpha) e_1(\alpha)^{-1} = \pm\alpha^j$ , вопреки предположению, что  $e_0(\alpha)$  не представима в виде  $\pm\alpha^j (1 - \sigma\alpha)^{y_1} (1 - \sigma^2\alpha)^{y_2} \dots (1 - \sigma^\mu\alpha)^{y_\mu}$ . Так как  $e(\alpha)^\lambda = (a_0 + a_1\alpha + \dots + a_{\lambda-1}\alpha^{\lambda-1})^\lambda \equiv a_0^\lambda + (a_1\alpha)^\lambda + \dots + (a_{\lambda-1}\alpha^{\lambda-1})^\lambda \equiv a_0 + a_1 + \dots + a_{\lambda-1} \equiv c \pmod{\lambda}$ , где  $c$  — целое число, отсюда следует, что существуют такие целые числа  $x_1, x_2, \dots, x_\mu$ , что  $x_1 + x_2 + \dots + x_\mu = 0$  и

$$\alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu} \equiv c \pmod{\lambda}, \quad (1)$$

но числа  $x_i$  не все делятся на  $\lambda$ . Остается доказать, что отсюда следует  $\lambda \mid (P/\lambda^{\mu-1})$ .

Было бы естественно попытаться перейти к логарифмам в соотношении (1), чтобы оно стало линейным соотношением относительно  $x_i$ , а точнее, несколькими линейными соотношениями, по одному для каждой степени  $\alpha$ . В то время как взятие логарифма представляется весьма далеким от сравнений в множестве круговых целых, понятие *логарифмической производной* ближе к алгебре, и оно-то действительно может быть применено к соотношению (1) следующим образом. Сначала запишем соотношение (1) в виде рационального соотношения для полиномов, заменив  $\alpha$  переменной  $X$ :

$$\begin{aligned} X^k (1 - \sigma X)^{x_1} (1 - \sigma^2 X)^{x_2} \dots (1 - \sigma^\mu X)^{x_\mu} = \\ = c + \lambda \Phi(X) + (1 + X + \dots + X^{\lambda-1}) \Psi(X), \end{aligned}$$

где  $\Phi(X)$ ,  $\Psi(X)$  — полиномы с целыми коэффициентами, а  $\sigma^\gamma X$  обозначает степень переменной  $X$  с показателем  $\gamma^j$  ( $\gamma$  — фиксированный примитивный корень по модулю  $\lambda$ ). Логарифмическая производная — это формальная алгебраическая операция, которую можно применить к обеим частям равенства и получить

$$\begin{aligned} \frac{k}{X} - x_1 \frac{\gamma\sigma X}{(1 - \sigma X) X} - x_2 \frac{\gamma^2\sigma^2 X}{(1 - \sigma^2 X) X} - \dots - x_\mu \frac{\gamma^\mu\sigma^\mu X}{(1 - \sigma^\mu X) X} = \\ = \frac{\lambda\Phi'(X) + (1 + X + \dots + X^{\lambda-1}) \Psi'(X) + (1 + 2X + \dots + (\lambda-1) X^{\lambda-2}) \Psi(X)}{c + \lambda\Phi(X) + (1 + X + \dots + X^{\lambda-1}) \Psi(X)}. \end{aligned}$$

Теперь положим  $X = \alpha$  в этом тождестве и умножим его на  $\alpha$ ; получим

$$\begin{aligned} k - x_1 \frac{\gamma\sigma\alpha}{1 - \sigma\alpha} - x_2 \frac{\gamma^2\sigma^2\alpha}{1 - \sigma^2\alpha} - \dots - x_\mu \frac{\gamma^\mu\sigma^\mu\alpha}{1 - \sigma^\mu\alpha} = \\ = \frac{\lambda\alpha\Phi'(\alpha) + \alpha(1 + 2\alpha + \dots + (\lambda-1)\alpha^{\lambda-2})\Psi(\alpha)}{e(\alpha)}. \end{aligned}$$

Правая часть этого равенства — корректно определенное круговое целое, поскольку  $e(\alpha)$  — единица. Ввиду того что первоначальное соотношение (1) было сравнением по модулю  $\lambda$  и из нового соотношения нельзя извлечь больше информации, чем оно содержало вначале, логично редуцировать последнее равенство по модулю  $\lambda$  и тем самым отбросить первый член числителя. Левую часть можно записать в виде

$$k - (x_1\gamma\sigma + x_2\gamma^2\sigma^2 + \dots + x_\mu\gamma^\mu\sigma^\mu) \left( \frac{\alpha}{1-\alpha} \right),$$

где полином  $x_1\gamma\sigma + x_2\gamma^2\sigma^2 + \dots + x_\mu\gamma^\mu\sigma^\mu$  от  $\sigma$  с целыми коэффициентами рассматривается обычным образом как отображение, ставящее в соответствие рациональным выражениям от  $\alpha$  с целыми коэффициентами другие рациональные выражения от  $\alpha$  с целыми коэффициентами. Все члены в левой части могут быть записаны со знаменателем  $\lambda$ , так что левая часть изобразится круговым целым, деленным на  $\lambda$ ; так как правая часть представляет собой круговое целое, то круговое целое, стоящее в числителе левой части, должно делиться на  $\lambda$ .

Выражение левой части как круговое целое, деленное на  $\lambda$ , можно быстро найти <sup>1)</sup> посредством дифференцирования полинома  $(X - 1)(X^{\lambda-1} + X^{\lambda-2} + \dots + X + 1) = X^\lambda - 1$  с последующей подстановкой  $X = \alpha$ . Тогда

$$(\alpha - 1)[(\lambda - 1)\alpha^{\lambda-2} + (\lambda - 2)\alpha^{\lambda-3} + \dots + 2\alpha + 1] = \lambda\alpha^{\lambda-1},$$

$$(\lambda - 1)\alpha^{\lambda-1} + (\lambda - 2)\alpha^{\lambda-2} + \dots + 2\alpha^2 + \alpha = \frac{\lambda}{\lambda - 1}.$$

Если перестроить степени  $\alpha^j$  в порядке  $\alpha, \sigma\alpha, \sigma^2\alpha, \dots$ , мы приходим к равенству

$$\alpha + \gamma\sigma\alpha + \gamma_2\sigma^2\alpha + \dots + \gamma_{\lambda-2}\sigma^{\lambda-2}\alpha = \frac{\lambda}{\alpha - 1},$$

где, как и раньше,  $0 < \gamma_j < \lambda$ ,  $\gamma_j \equiv \gamma^j \pmod{\lambda}$ . Тогда

$$\frac{\alpha}{\alpha - 1} = \frac{1}{1 - \alpha^{-1}} = -\sigma^\mu \left( \frac{1}{\alpha - 1} \right) = -\frac{\sigma^\mu}{\lambda} (\alpha + \gamma_1\sigma\alpha + \dots + \gamma_{\lambda-2}\sigma^{\lambda-2}\alpha).$$

Выражение в скобках можно переписать в виде  $\varphi(\sigma)(\alpha)$ , где, как и раньше,  $\varphi(X) = 1 + \gamma_1X + \gamma_2X^2 + \dots + \gamma_{\lambda-2}X^{\lambda-2}$ , а  $\varphi(\sigma)$  — отображение круговых целых в круговые целые. Таким образом, соотношение принимает вид

$$\begin{aligned} k + (x_1\gamma\sigma + x_2\gamma^2\sigma^2 + \dots + x_\mu\gamma^\mu\sigma^\mu) \frac{\sigma^\mu}{\lambda} \varphi(\sigma)(\alpha) &\equiv \\ &\equiv e(\alpha)^{-1} \Psi(\alpha) [\lambda/(\alpha - 1)] \pmod{\lambda}. \end{aligned}$$

<sup>1)</sup> Другой вывод см. в упр. 11 к § 4.4.

Для того чтобы представить круговое целое  $e(\alpha)^{-1}\Psi(\alpha)$  в виде  $q(\alpha)(\alpha - 1) + a$  при некотором целом числе  $a$ , можно воспользоваться делением полиномов. Тогда правая часть становится равной  $\lambda q(\alpha) + a[\lambda/(\alpha - 1)] \equiv a[\lambda/(\alpha - 1)] \equiv a\varphi(\sigma)(\alpha) \pmod{\lambda}$ . Значит,

$$k + \frac{\sigma^\mu}{\lambda} (x_1\gamma\sigma + x_2\gamma^2\sigma^2 + \dots + x_\mu\gamma^\mu\sigma^\mu) \varphi(\sigma)(\alpha) \equiv a\varphi(\sigma)(\alpha) \pmod{\lambda}.$$

Для ликвидации в левой части знаменателя  $\lambda$  можно применить к обеим частям оператор  $\gamma\sigma - 1$  и, используя определяющее соотношение  $(\gamma X - 1)\varphi(X) = \lambda\psi(X) + (X^{\lambda-1} - 1)$  для  $\psi(X)$ , найти

$$\begin{aligned} \gamma k - k + \sigma^\mu (x_1\gamma\sigma + x_2\gamma^2\sigma^2 + \dots + x_\mu\gamma^\mu\sigma^\mu) \psi(\sigma)(\alpha) &\equiv \\ &\equiv a\lambda\psi(\sigma)(\alpha) \equiv 0 \pmod{\lambda}, \end{aligned}$$

ибо  $\sigma^{\lambda-1} - 1$  все переводит в 0. Это показывает, что применение оператора

$$(x_1\gamma\sigma + x_2\gamma^2\sigma^2 + \dots + x_\mu\gamma^\mu\sigma^\mu) \psi(\sigma) \quad (2)$$

к  $\alpha$  дает целое число по модулю  $\lambda$ , которое мы обозначим через  $K$ . Тогда применение того же самого оператора к  $\sigma^j\alpha$  дает  $\sigma^j K = K$  по модулю  $\lambda$  для всех  $j$ . Теперь нужно показать, что если это верно и если не все  $x_i$  по модулю  $\lambda$  равны нулю, то  $\lambda \mid (P/\lambda^{\mu-1})$ .

Это позволяет сделать конечномерный анализ Фурье по модулю  $\lambda$  (см. § 6.9). Заметим, что имеется  $\lambda^{\lambda-1}$  различных круговых целых по модулю  $\lambda$  и каждое из них может быть записано точно одним способом по модулю  $\lambda$  в виде линейной комбинации (с целыми коэффициентами по модулю  $\lambda$ ) от  $\lambda - 1$  круговых целых

$$\alpha + \gamma^j\sigma\alpha + \gamma^{2j}\sigma^2\alpha + \dots + \gamma^{-j}\sigma^{-1}\alpha,$$

где  $j = 0, 1, \dots, \lambda - 2$ . Это доказывается точно так же, как и раньше, при помощи формулы обращения Фурье  $(1 + \gamma^{j-1} + \gamma^{2(j-k)} + \dots + \gamma^{-(j-k)}) \equiv 0 \pmod{\lambda}$ , кроме случая  $j \equiv k \pmod{\lambda - 1}$ , а если  $j \equiv k \pmod{\lambda - 1}$ , то это же самое  $\equiv (\lambda - 1) \not\equiv 0 \pmod{\lambda}$ .

Применение оператора  $\sigma$  к круговому целому  $\alpha + \gamma^j\sigma\alpha + \dots + \gamma^{-j}\sigma^{-1}\alpha$  умножает его на  $\gamma^{-j}$  по модулю  $\lambda$ . Значит, применение оператора (2) к этому круговому целому умножает его на

$$(x_1\gamma^{1-j} + x_2\gamma^{2(1-j)} + \dots + x_\mu\gamma^{\mu(1-j)}) \psi(\gamma^{-j}). \quad (3)$$

С другой стороны, применение оператора (2) к  $\alpha + \gamma^j\sigma\alpha + \dots + \gamma^{-j}\sigma^{-1}\alpha$  переводит его в  $K + \gamma^j K + \dots + \gamma^{-j} K = K(1 + \gamma^j + \dots + \gamma^{-j}) \equiv 0 \pmod{\lambda}$  при  $j = 1, 2, \dots, \lambda - 2$ . Значит, целое число (3) должно быть нулем по модулю  $\lambda$  при  $j = 1, 2, \dots, \lambda - 2$ .

В предыдущем параграфе было показано, что  $\lambda$  тогда и только тогда делит числитель числа  $B_{n+1}$ , когда  $\psi(\gamma^n) \equiv 0 \pmod{\lambda}$ .



Значит, если  $\lambda$  не делит числители чисел  $B_2, B_4, \dots, B_{\lambda-3}$ , то второй сомножитель  $\psi(\gamma^{-j})$  в (3) отличен от нуля по модулю  $\lambda$  в  $\mu - 1$  случаях  $j = -1, -3, -5, \dots, -\lambda + 4$ . Кроме того, как было показано в предыдущем параграфе,  $\psi(\gamma^{\lambda-2}) \not\equiv 0 \pmod{\lambda}$ . Это дает  $\mu$  сравнений

$$x_1 \gamma^{j+1} + x_2 \gamma^{2j+2} + \dots + x_\mu \gamma^{\mu j + \mu} \equiv 0 \pmod{\lambda},$$

где  $j = 1, 3, 5, \dots, \lambda - 2$ . Решая их при помощи обращения Фурье, найдем  $x_i \equiv 0 \pmod{\lambda}$  при  $i = 1, 2, \dots, \mu$ . Таким образом, если  $x_i \not\equiv 0 \pmod{\lambda}$  при некотором  $i$ , то  $\lambda$  должно делить числитель по крайней мере одного из чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$ , и теорема доказана.

## Упражнения

1. Покажите, что если число элементов группы не делится на  $\lambda$ , то каждый элемент этой группы (записанной мультипликативно) есть  $\lambda$ -я степень.

2. Покажите, что если  $e_2(\alpha)$  есть такая единица, что  $e_2(\alpha)^\lambda = \pm \alpha^k$ , то  $e_2(\alpha) = \pm \alpha^j$ .

3. Доказательство Куммера того, что если  $\lambda \mid h_2$ , то имеется единица, непредставимая в виде  $\pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$ , но  $\lambda$ -я степень которой представима в этом виде, строится примерно следующим образом. Заполните в нем детали.

Пусть  $\Lambda_1$  обозначает решетку всех точек вида  $\Phi(e(\alpha))$  в пространстве переменных  $x_1, x_2, \dots, x_\mu$ . Здесь  $e(\alpha)$  пробегает все единицы, а  $\Phi$  было определено в § 6.10. Пусть  $\Lambda_2 \subseteq \Lambda_1$  — подрешетка, состоящая из тех точек решетки  $\Lambda_1$ , все координаты которых целые, или, что то же самое, из  $\Phi$ -образов единиц, эквивалентных единице 1. Точки  $v_1 = (1, -1, 0, \dots, 0)$ ,  $v_2 = (0, 1, -1, 0, \dots, 0)$ ,  $\dots$ ,  $v_{\mu-1} = (0, 0, \dots, 0, 1, -1)$  образуют базис в  $\Lambda_2$ . На основании элементарной линейной алгебры в  $\Lambda_1$  имеется базис  $w_1, w_2, \dots, w_{\mu-1}$  и каждое из  $w_i$  может быть точно одним способом записано в виде  $w_i = \sum c_{ij} v_j$ , где  $c_{ij}$  — рациональные числа. Так как одна из каждой  $h_2$  единиц эквивалентна единице 1, то  $\det(c_{ij}) = 1/h_2$ . Пусть  $n_i$  — наименьший общий знаменатель для чисел  $c_{ij}$  при  $j = 1, 2, \dots, \mu - 1$ . Тогда  $\det(c_{ij})$  есть целое число, деленное на произведение всех  $n_i$ . Если это число есть  $1/h_2$  и  $\lambda \mid h_2$ , то отсюда следует, что  $\lambda \mid n_i$  по крайней мере для одного  $i$ . Если  $e(\alpha)$  — единица, для которой  $\Phi e(\alpha) = w_i$ , то  $e(\alpha)^{n_i}$  — единица, эквивалентная единице 1. С другой стороны,  $\lambda \mid n_i$  и единица  $e(\alpha)^{n_i/\lambda}$  не эквивалентна единице 1, так как иначе  $n_i/\lambda$  было бы общим знаменателем для чисел  $c_{ij}$ .

4. Докажите, что если  $G$  — абелева группа, порядок которой делится на простое число  $p$ , то она содержит элемент порядка  $p$ .

## 6.18. Лемма Куммера

Как уже было показано, куммерово условие (A) эквивалентно условию, что  $\lambda$  не делит числители чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$ . Чтобы доказать Последнюю теорему Ферма для тех простых чисел  $\lambda$ , которые удовлетворяют этому условию, остается

только доказать, что, как и предполагал Куммер, из (А) вытекает (В). Это утверждение известно как *лемма Куммера*. Доказательство представляет собой короткое добавление к рассуждениям предыдущего параграфа.

В предыдущем параграфе было показано, что если  $e(\alpha)$  — единица вида  $\pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$  и  $e(\alpha) \equiv c \pmod{\lambda}$ , где  $c$  — целое число, то либо условие (А) не выполняется, либо все целые числа  $x_1, x_2, \dots, x_\mu$  делятся на  $\lambda$ . Далее, если  $e(\alpha)$  — любая единица, то  $e(\alpha)^{h_2}$  имеет вид  $\pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$ . Это следует из доводов, использованных в доказательстве теоремы Ферма и нескольких ее аналогов, приведенных в этой книге (см. упр. 2), поскольку  $h_2$  является, по определению, числом единиц, различных по модулю единиц специального вида. Предположим теперь, что условие (А) выполняется и что  $e(\alpha) \equiv c \pmod{\lambda}$ . Тогда  $e(\alpha)^{h_2} = \pm \alpha^k (1 - \sigma\alpha)^{x_1} (1 - \sigma^2\alpha)^{x_2} \dots (1 - \sigma^\mu\alpha)^{x_\mu}$  и  $e(\alpha)^{h_2} \equiv c^{h_2} \pmod{\lambda}$ , и, следовательно, все числа  $x_1, x_2, \dots, x_\mu$  делятся на  $\lambda$ . Значит,  $e(\alpha)^{h_2} = \pm \alpha^k e_0(\alpha)^\lambda$  для некоторой единицы  $e_0(\alpha)$ . Кроме того,  $h_2$  не делится на  $\lambda$  (по условию (А) и потому, что  $2^{\mu-1}h_1$  — целое число) и существуют такие целые числа  $a$  и  $b$ , что  $ah_2 + b\lambda = 1$ . Таким образом,  $e(\alpha) = e(\alpha)^{ah_2} e(\alpha)^{b\lambda} = (\pm \alpha^k)^a e_0(\alpha)^{a\lambda} e(\alpha)^{b\lambda}$ . Это показывает, что  $\alpha^{ak}$  сравнимо по модулю  $\lambda$  с целым числом, откуда следует, что  $ak \equiv 0 \pmod{\lambda}$ ,  $\alpha^{ak} = 1$  (упр. 1). Итак,  $e(\alpha) = [e_0(\alpha)^a e(\alpha)^b]^\lambda$ , или  $e(\alpha) = [-e_0(\alpha)^a e(\alpha)^b]^\lambda$ . Таким образом, из условия (А) и сравнения  $e(\alpha) \equiv c \pmod{\lambda}$  вытекает, что  $e(\alpha)$  есть  $\lambda$ -я степень. Это и доказывает лемму Куммера.

## Упражнения

1. Докажите, что если  $\alpha^j$  сравнимо с целым числом по модулю  $\lambda$ , то  $j \equiv 0 \pmod{\lambda}$ . [Запишите  $\alpha = 1 - (1 - \alpha)$ .]
2. Пусть задана группа, число элементов которой равно  $h$ , и пусть  $b$  — элемент этой группы. Покажите, что если  $d$  — число различных степеней элемента  $b$ , то элементы группы можно разбить на подмножества, содержащие по  $d$  элементов каждое. Выведите отсюда, что  $d$  делит  $h$  и что  $b^h$  есть единица группы.

## 6.19. Краткие выводы

Итак, в этой главе доказано, что простое число  $\lambda$  тогда и только тогда удовлетворяет куммеровым условиям (А) и (В) (т. е. является регулярным), когда оно не делит числитель никакого из чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$ . Как показано в гл. 5, для таких простых чисел Последняя теорема Ферма верна. При помощи результата этой главы уже становится делом стандартного подсчета доказательство того, например, что Последняя теорема

Ферма верна для всех простых показателей, меньших 100, исключая, возможно, показатели 37, 59, 67. (А отсюда следует, что она верна для всех показателей, простых или нет, меньших 100, исключая, возможно, эти три, а также показатель 74.)

Вначале Куммер сделал поспешный вывод, что регулярных простых чисел бесконечно много, но позже он осознал, что не может этого доказать. Хотя ясно, как из опыта, так и из теоретических соображений, что около 60% всех простых чисел регулярны (см. [J4]), тем не менее и по сей день не доказано, что множество регулярных простых чисел бесконечно. (По иронии судьбы, сравнительно легко доказать, что иррегулярных простых чисел бесконечно много — см. [B2].)

Конечно, из теоремы Куммера не вытекает, что Последняя теорема Ферма нарушается для 37, 59 и 67. Ясно лишь, что ее доказательство требует более мощной техники и понимания еще более тонких свойств арифметики круговых целых, построенных из корней 37-й, 59-й или 67-й степени из единицы. Такую технику развивали сам Куммер, а в дальнейшем Мириманов, Виферих, Фуртвенглер, Вандивер и многие другие. Это продолжение работы Куммера станет темой предполагаемого второго тома этой книги. Сейчас же достаточно сказать, что Последняя теорема Ферма была доказана для всех показателей вплоть до нескольких тысяч (см. [W1]), но большинство критериев справедливости теоремы оставляют желать много лучшего. Например, еще не доказано, что Последняя теорема Ферма верна для бесконечного множества простых показателей.

## ТЕОРИЯ ДИВИЗОРОВ КВАДРАТИЧНЫХ ЦЕЛЫХ

## 7.1. Простые дивизоры

Эта глава посвящена изучению того, что, возможно, имел в виду Куммер, когда говорил об идеальных комплексных числах вида  $x + y \sqrt{D}$  (см. § 5.1). Основная задача при создании этой теории состоит в определении понятия *простого дивизора* чисел  $x + y \sqrt{D}$ , или, как сказал бы Куммер, понятия идеального простого числа такого вида. Как и в гл. 4, воспользуемся следующим методом: будем предполагать, что такое понятие существует, и из этого предположения выводить следствия о том, каким оно должно быть. Однако при этом окажется, что для того, чтобы полученная теория «работала», нам придется несколько пересмотреть и понятие «комплексных чисел вида  $x + y \sqrt{D}$ ».

Пусть  $D$  — фиксированное целое; рассмотрим множество всех чисел вида  $x + y \sqrt{D}$  с целыми  $x$  и  $y$ . Естественно исключить из рассмотрения случаи  $D = 0$  и  $D = 1$ , поскольку тогда  $x + y \sqrt{D}$  является обыкновенным целым числом. Кроме того, если  $D$  делится на квадрат, скажем  $D = t^2 D'$ , то  $x + y \sqrt{D} = x + ty \sqrt{D'}$ , и числа  $x + y \sqrt{D}$  содержатся среди чисел вида  $x + y \sqrt{D'}$ . Как будет показано в § 8.1, отсюда не следует, что теория дивизоров чисел вида  $x + y \sqrt{D}$  полностью сводится к теории дивизоров чисел вида  $x + y \sqrt{D'}$ . Однако это означает, что между этими теориями имеется очень тесная связь; поэтому разумно рассмотреть сначала случай *свободного от квадратов*  $D$ , т. е.  $D$ , не равного 0 или 1 и не делящегося ни на один квадрат, отличный от 1. Эта глава посвящена исключительно случаю  $D$ , свободного от квадратов.

Ясно, как складывать и умножать числа вида  $x + y \sqrt{D}$ . Эти две операции удовлетворяют коммутативному, ассоциативному и дистрибутивному законам и определяют арифметику (*кольцо* — в терминологии современной алгебры) с обычными свойствами. В частности, в этом множестве возможно *вычитание*, т. е. уравнение  $a + X = b$  имеет единственное решение  $X$  для любой пары чисел вида  $a = x + y \sqrt{D}$ ,  $b = x' + y' \sqrt{D}$ . Действительно,  $X = (x' - x) + (y' - y) \sqrt{D}$ . Деление обычно невы-

полнимо, но существует мультипликативная единица 1 ( $1 \cdot a = a$  для всех  $a$ ) и обе части равенства можно сокращать на ненулевые множители, т. е. из  $ab = ac$  и  $a \neq 0$  следует, что  $b = c$ . Для доказательства последнего утверждения необходимо и достаточно доказать, что если  $(x + y \sqrt{D}) \cdot (x' + y' \sqrt{D}) = 0 + 0 \sqrt{D}$  и  $x + y \sqrt{D} \neq 0 + 0 \sqrt{D}$ , то  $x' + y' \sqrt{D} = 0 + 0 \sqrt{D}$ . Для этого умножим обе части первого равенства на  $x - y \sqrt{D}$ ; тогда мы получим  $(x^2 - Dy^2)(x' + y' \sqrt{D}) = 0 + 0 \sqrt{D}$ . Отсюда следует, что  $(x^2 - Dy^2)x' = 0$ ,  $(x^2 - Dy^2)y' = 0$ , и если  $x^2 - Dy^2 \neq 0$ , то мы приходим к требуемому заключению. Поскольку из  $x^2 = Dy^2$  следует<sup>1)</sup>, что  $D$  является квадратом (при условии  $y \neq 0$ ), то нужное нам заключение получается из предположения о том, что  $D$  свободно от квадратов.

Для чисел вида  $x + y \sqrt{D}$  можно определить операцию *сопряжения*: она переводит  $x + y \sqrt{D}$  в  $x - y \sqrt{D}$ . Произведение всех сопряженных к данному элементу  $x + y \sqrt{D}$  инвариантно относительно сопряжения и, следовательно, является обыкновенным целым числом. Точнее,  $(x + y \sqrt{D})(x - y \sqrt{D}) = x^2 - Dy^2$ . Это целое называется *нормой*  $x + y \sqrt{D}$ . Использование нормы позволяет (как и для круговых целых в § 4.2) свести деление на числа вида  $x + y \sqrt{D}$  к делению на обычные целые. Действительно, утверждение, что  $x + y \sqrt{D}$  делит  $u + v \sqrt{D}$  и дает частное  $r + s \sqrt{D}$ , равносильно утверждению, что целое  $x^2 - Dy^2$  делит  $(u + v \sqrt{D})(x - y \sqrt{D})$  и дает частное  $r + s \sqrt{D}$ . (В элементарной алгебре это называется «освобождением от иррациональности в знаменателе».) Поскольку  $D$  не является квадратом, норма  $x^2 - Dy^2$  не равна нулю, если сам элемент  $x + y \sqrt{D}$  отличен от нуля. Однако в отличие от ситуации с круговыми целыми при  $D > 0$  нормы могут быть отрицательными.

Для построения теории дивизоров в такой арифметике чисел вида  $x + y \sqrt{D}$  воспользуемся методом *анализа* из § 4.3 и 4.6. А именно, предположим, что можно определить простые дивизоры, обладающие ожидаемыми свойствами, и из этого предположения выведем *необходимые* условия для существования теории дивизоров. Мы получим достаточно необходимых условий для того, чтобы точно определить, какими должны быть простые дивизоры и как ввести понятие делимости на простой дивизор (с кратностями). Затем в § 7.2 последует *синтез*, при котором будет показано, что найденные необходимые условия являются также и *достаточными*, т. е. если использовать их для построения тео-

<sup>1)</sup> См. предложение из § 1.3.

рии дивизоров, то полученная теория будет свободна от противоречий и обладать ожидаемыми свойствами.

На первом этапе анализа заметим, что для любого простого дивизора  $A$  найдется единственное положительное целое  $p$ , обладающее тем свойством, что обыкновенные целые (элементы вида  $x + 0 \sqrt{D}$ ) делятся на  $A$  тогда и только тогда, когда они делятся на  $p$ . Действительно, дивизор  $A$  должен делить некоторое  $x + y \sqrt{D}$ , а следовательно, и его норму  $N(x + y \sqrt{D}) = (x + y \sqrt{D})(x - y \sqrt{D}) = x^2 - Dy^2$ . Поэтому  $A$  делит  $|x^2 - Dy^2|$ . Это число является положительным целым; следовательно, его можно записать в виде произведения положительных простых. (Частный случай  $|x^2 - Dy^2| = 1$  невозможен, поскольку тогда  $A$  делил бы 1, а тем самым и все квадратичные целые.) Из предположения о том, что  $A$  является *простым* дивизором (если он делит произведение, то он делит один из сомножителей), следует, что  $A$  делит по крайней мере одно простое положительное целое число, скажем  $A \mid p$ . Произвольное целое число  $x$  можно записать в виде  $x = qp + r$ ,  $0 \leq r < p$ . Если  $r = 0$ , то  $A$  делит  $x$ . Обратно, если  $r \neq 0$ , то  $r$  и  $p$  взаимно просты и существует целое  $y$ , сравнимое с 0 по модулю  $p$  и с 1 по модулю  $r$ ; если бы дивизор  $A$  делил  $x$ , то он делил бы как  $r$ , так и  $y = nr + 1$ , т. е.  $A$  делил бы 1, что невозможно. Это доказывает, что  $A$  делит  $x$  тогда и только тогда, когда  $p$  делит  $x$ . В частности,  $p$  — единственное простое положительное целое, делящееся на  $A$ .

Если бы  $\sqrt{D} (= 0 + 1 \sqrt{D})$  был сравним с каким-либо целым по модулю  $A$  (т. е. если бы  $r - \sqrt{D}$  делилось на  $A$  для некоторого целого  $r$ ), то каждый элемент  $x + y \sqrt{D}$  был бы сравним с целым числом по модулю  $A$ . Поскольку можно установить, когда два целых числа сравнимы по модулю  $A$ , тогда можно было бы и сказать, когда два числа вида  $x + y \sqrt{D}$  сравнимы по модулю  $A$ . Следовательно, естественно попытаться определить, сравним ли  $\sqrt{D}$  с каким-либо целым по модулю  $A$ . Поскольку  $A$  — простой дивизор,  $\sqrt{D}$  сравним с каким-либо целым по модулю  $A$  тогда и только тогда, когда  $(\sqrt{D} - 1)(\sqrt{D} - 2) \dots (\sqrt{D} - p)$  делится на  $A$ . Согласно обобщению теоремы Ферма, доказанному в § 4.6,  $(X - 1)(X - 2) \dots (X - p) \equiv X^p - X \pmod{p}$ . Следовательно,  $(\sqrt{D} - 1)(\sqrt{D} - 2) \dots (\sqrt{D} - p) \equiv \sqrt{D}(\sqrt{D}^{p-1} - 1) \pmod{A}$ . Это показывает, что  $\sqrt{D}$  сравним с каким-либо целым по модулю  $A$  тогда и только тогда, когда  $\sqrt{D} \equiv 0 \pmod{A}$  или  $\sqrt{D}^{p-1} \equiv 1 \pmod{A}$ .

Сначала рассмотрим случай, когда  $\sqrt{D} \equiv 0 \pmod{A}$ . Если предположить, что дивизоры имеют *нормы* (т. е. что существует целое, дивизор которого равен произведению сопряженных к  $A$ ),



то норма  $A$  должна делить как  $D = -N(\sqrt{D})$ , так и  $p^2 = N(p)$ . Следовательно, норма  $A$  равна либо 1, либо  $p$  (поскольку  $D$  свободно от квадратов); но если бы норма  $A$  была равна 1, то  $A$  делил бы 1, поэтому норма  $A$  должна быть равна  $p$ . Далее,  $A$  делит  $\sqrt{D}$  и  $D = p \cdot k$ , где  $k$  — целое, не делящееся на  $p$ . Таким образом,  $A^2$  делит  $(\sqrt{D})^2 = pk$ , и поскольку  $A$  вообще не делит  $k$ , то  $A^2$  делит  $p$ . С другой стороны,  $N(A^2) = N(A)^2 = p^2 = N(p)$ . Следовательно,  $A^2$  является дивизором  $p$ ,  $A$  делит  $p$  с кратностью точно 2 и  $A$  делит  $\sqrt{D}$  с кратностью точно 1. Таким образом, дивизор  $A$  делит  $x + y\sqrt{D}$  с кратностью  $\mu$  тогда и только тогда, когда он делит  $(x + y\sqrt{D})(\sqrt{D})^\mu$  с кратностью  $2\mu$ , что справедливо в том и только в том случае, когда  $p^\mu$  делит  $(x + y\sqrt{D})(\sqrt{D})^\mu$ . Поскольку последнее условие имеет смысл в арифметике чисел вида  $x + y\sqrt{D}$  без каких-либо предположений о дивизорах, его можно взять в качестве *определения* делимости на простой дивизор  $A$  числа  $p$ .

**Определение.** Если  $p$  делит  $D$ , то  $p$  имеет один простой дивизор  $A$ , и  $A$  делит  $x + y\sqrt{D}$  с кратностью  $\mu$ , если  $p^\mu$  делит  $(x + y\sqrt{D})(\sqrt{D})^\mu$ .

Теперь рассмотрим случай, когда  $(\sqrt{D})^{p-1} \equiv 1 \pmod{A}$ . Случай  $p = 2$  будет рассмотрен ниже. Для простых  $p$ , отличных от 2, число  $(\sqrt{D})^{p-1}$  является *обыкновенным целым*, поскольку  $p - 1$  четно. Если  $p$  — простое, для которого это целое сравнимо с 1 по модулю  $p$ , то, как было показано выше, для любого простого дивизора  $A$  числа  $p$  найдется такое целое  $u$ , что  $\sqrt{D} \equiv u \pmod{A}$ . Если задан такой дивизор  $A$ , то сопряженный к нему, который мы будем обозначать  $\bar{A}$ , также является простым дивизором  $p$ , и так как  $A$  делит  $u - \sqrt{D}$ , то  $\bar{A}$  делит  $u + \sqrt{D}$ , т. е.  $\sqrt{D} \equiv -u \pmod{\bar{A}}$ . Отсюда следует, что  $\bar{A}$  отличен от  $A$ . Действительно, из равенства  $A = \bar{A}$  следовало бы, что  $u \equiv -u \pmod{A}$ ,  $2u \equiv 0 \pmod{p}$ , и потому либо  $2 = p$ , либо  $(\sqrt{D})^{p-1} \equiv u^{p-1} \equiv 0 \pmod{p}$ , что противоречит нашему предположению. Таким образом,  $A$  и  $\bar{A}$  различны и оба делят  $p$ . Поскольку норма  $p$  равна  $p^2$ , а нормы как  $A$ , так и  $\bar{A}$  равны некоторой степени  $p$ , отсюда следует, что нормы  $A$  и  $\bar{A}$  должны быть равны  $p$  и каждый из этих дивизоров должен делить  $p$  с кратностью 1, а  $A\bar{A}$  должен быть дивизором  $p$ . Так как  $A$  не делит  $u + \sqrt{D}$ , то  $A$  делит  $x + y\sqrt{D}$  с кратностью  $\mu$  тогда и только тогда, когда он делит  $(x + y\sqrt{D}) \times \times (u + \sqrt{D})^\mu$  с кратностью  $\mu$ . Согласно основной теореме, это

справедливо в том и только в том случае, когда  $p^\mu$  делит  $(x + y\sqrt{D})(u + \sqrt{D})^\mu$ . Аналогично,  $\bar{A}$  делит  $x + y\sqrt{D}$  с кратностью  $\mu$  тогда и только тогда, когда  $p^\mu$  делит  $(x + y\sqrt{D})(u - \sqrt{D})^\mu$ . Как только целое число  $u$  найдено, мы можем принять это в качестве *определения* дивизоров  $A$  и  $\bar{A}$ .

Выше было показано, что если  $p$  имеет простой дивизор  $A$ , то  $\sqrt{D} \equiv u \pmod{A}$  для некоторого целого  $u$ ; отсюда следует, что сравнение  $u^2 \equiv D \pmod{p}$  разрешимо для этого  $p$ . К такому же заключению можно прийти, не привлекая теории дивизоров: для этого достаточно положить  $X = \sqrt{D}$  в  $(X - 1)(X - 2) \dots (X - p + 1) \equiv X^{p-1} - 1$ , и, взяв нормы от обеих частей сравнения, получить  $(1^2 - D)(2^2 - D) \dots ((p-1)^2 - D) \equiv \equiv 0 \pmod{p}$  (поскольку по предположению  $\sqrt{D}^{p-1} \equiv 1 \pmod{p}$ ). Таким образом,  $D \equiv u^2 \pmod{p}$  по крайней мере для одного значения  $u = 1, 2, \dots, p-1$ . Если  $D \equiv u^2$  и  $D \equiv v^2 \pmod{p}$ , то  $(u - v)(u + v) = u^2 - v^2 \equiv 0 \pmod{p}$ . Отсюда следует, что  $u \equiv \pm v \pmod{p}$ . Поскольку  $u \not\equiv -u \pmod{p}$  ( $p \neq 2$  и  $u^2 \not\equiv 0 \pmod{p}$ ), это доказывает, что для *нечетных простых*  $p$ , которые удовлетворяют сравнению  $\sqrt{D}^{p-1} \equiv 1 \pmod{p}$ , существуют ровно два различных решения по модулю  $p$  сравнения  $u^2 \equiv D \pmod{p}$ .

**Определение.** Если  $p \neq 2$  и  $D^{(p-1)/2} \equiv 1 \pmod{p}$ , то существуют в точности два решения  $u$  по модулю  $p$  сравнения  $u^2 \equiv D \pmod{p}$ . Для каждого из этих решений  $u$  определим простой дивизор  $A$  числа  $p$  условием:  $A$  делит  $x + y\sqrt{D}$  с кратностью  $\mu$ , если  $p^\mu$  делит  $(x + y\sqrt{D}) \cdot (\sqrt{D} + u)^\mu$ .

Простые дивизоры других простых  $p \neq 2$  выглядят даже проще. Действительно, если  $p \neq 2$ ,  $D \not\equiv 0 \pmod{p}$  и  $D^{(p-1)/2} \not\equiv 1 \pmod{p}$ , то само  $p$  является простым. Легко видеть, что так и должно быть, поскольку  $p$  должно иметь какой-то простой дивизор  $A$  (иначе условие делимости на  $p$  было бы бессодержательным и  $p$  должно было бы делить 1), и если этот простой дивизор не равен самому  $p$ , то он делит некоторый элемент вида  $x + y\sqrt{D}$ , который *не* делится на  $p$ . Если бы  $p$  делило  $y$ , то, поскольку  $A$  делит  $x + y\sqrt{D}$  и, значит,  $p$  делит  $x^2 - Dy^2$ , отсюда следовало бы, что  $p$  делит  $x$  и что  $p$  делит  $x + y\sqrt{D}$ , но это противоречит предположению. Таким образом, если  $p$  не является простым, то оно имеет простой дивизор, который делит некоторый элемент вида  $x + y\sqrt{D}$  с  $y \not\equiv 0 \pmod{p}$ . Тогда  $-x \equiv y\sqrt{D} \pmod{A}$  и существует такое целое  $z$ , что  $yz \equiv 1 \pmod{p}$ . Отсюда следует, что  $\sqrt{D}$  должен быть сравним с некоторым целым по модулю  $A$ , а именно с  $-zx$ . Поэтому, как показано выше,  $D \equiv 0 \pmod{p}$  или  $D^{(p-1)/2} \equiv$

$\equiv 1 \pmod{p}$ . Если  $p$  не удовлетворяет ни одному из этих условий и если теория дивизоров возможна, то само  $p$  должно быть простым, т. е. произведение  $(x + y \sqrt{D})(u + v \sqrt{D})$  делится на  $p$ , только если один из множителей делится на  $p$ .

Для того чтобы доказать, что  $p$  — простое, необходимо и достаточно (упр. 1) доказать, что если  $p$  делит норму  $x^2 - Dy^2$  числа  $x + y \sqrt{D}$ , то  $p$  делит  $x + y \sqrt{D}$ . Пусть  $n = D^{(p-1)/2}$  (мы по-прежнему предполагаем, что  $p \neq 2$ , поэтому  $n$  — целое). Тогда  $n^2 = D^{p-1}$ , и, согласно теореме Ферма и предположению  $D \not\equiv 0 \pmod{p}$ , мы получаем, что  $n^2 \equiv 1 \pmod{p}$ . Таким образом,  $(n+1)(n-1) \equiv 0 \pmod{p}$ , и из предположения  $n \not\equiv 1 \pmod{p}$  следует, что  $n \equiv -1 \pmod{p}$ . Если  $p$  делит  $x^2 - Dy^2$ , то  $x^2 \equiv Dy^2 \pmod{p}$ ; возводя обе части этого сравнения в  $(p-1)/2$ -ю степень, мы получим, что  $x^{p-1} \equiv ny^{p-1}$ ,  $x^{p-1} + y^{p-1} \equiv 0 \pmod{p}$ . Согласно теореме Ферма,  $x^{p-1}$  и  $y^{p-1}$  по модулю  $p$  может быть равно только 0 или 1, и так как  $p \neq 2$ , то сравнение  $x^{p-1} + y^{p-1} \equiv 0 \pmod{p}$  может выполняться только при  $x^{p-1} \equiv y^{p-1} \equiv 0$ . Отсюда следует, что  $x \equiv 0, y \equiv 0 \pmod{p}$ , т. е.  $p$  делит  $x + y \sqrt{D}$ , что и требовалось доказать.

**Определение.** Если  $p \neq 2$ ,  $D^{(p-1)/2} \equiv -1 \pmod{p}$ , то единственным простым дивизором  $p$  является дивизор, определенный условием: « $A$  делит  $x + y \sqrt{D}$  с кратностью  $\mu$ , если  $p^\mu$  делит  $x + y \sqrt{D}$ ».

Теперь нам остается только найти простые дивизоры числа 2 в случае  $D \not\equiv 0 \pmod{p}$ , т. е. при нечетном  $D$ . В этом случае  $1 - D = (1 - \sqrt{D})(1 + \sqrt{D})$  делится на 2; поэтому любой простой дивизор числа 2 должен делить либо  $1 - \sqrt{D}$ , либо  $1 + \sqrt{D}$ , т. е. если  $A$  — произвольный простой дивизор числа 2, то  $\sqrt{D} \equiv \pm 1 \pmod{A}$ . Так как  $1 \equiv -1 \pmod{2}$ , то эти два случая совпадают и  $\sqrt{D}$  должен быть сравним с 1 по модулю  $A$ . Следовательно,  $A$  делит  $1 - D = (1 - \sqrt{D})(1 + \sqrt{D})$  с кратностью, не меньшей 2. Если  $1 - D = 2k$ , где  $k$  нечетно, т. е. если  $D \equiv 3 \pmod{4}$ , то  $A$  делит 2 с кратностью, не меньшей 2. С другой стороны,  $N(A)$  равна 2 или 4, так как она делит  $N(2) = 4$  и отлична от 1. Если  $A^2$  делит 2, то не только  $N(A) = 2$ , но и  $A^2$  является дивизором 2. Действительно, частное от деления дивизора 2 на  $A^2$  имеет норму  $N(2)/N(A^2) = 4/N(A)^2 \leq 1$ . Таким образом, если  $D \equiv 3 \pmod{4}$ , то  $A$  делит  $1 - \sqrt{D}$  и  $1 + \sqrt{D}$  с кратностью точно 1, и  $A$  делит  $x + y \sqrt{D}$  с кратностью  $\mu$  тогда и только тогда, когда  $2^\mu$  делит  $(x + y \sqrt{D})(1 - \sqrt{D})^\mu$ .

**Определение.** Если  $D \equiv 3 \pmod{4}$ , то 2 имеет единственный простой дивизор  $A$ , и  $A$  делит  $x + y \sqrt{D}$  с кратностью  $\mu$ , если  $2^\mu$  делит  $(x + y \sqrt{D})(1 - \sqrt{D})^\mu$ .

Теперь нам остается рассмотреть только простые дивизоры числа 2 при  $D \equiv 1 \pmod{4}$ . Однако в этом случае мы приходим к противоречию. Пусть  $A$  — простой дивизор числа 2. Тогда, как и в случае  $D \equiv 3 \pmod{4}$ ,  $\sqrt{D} \equiv 1 \pmod{A}$  и  $A$  делит  $x + y \sqrt{D}$  в том и только в том случае, если он делит  $x + y$ , а последнее имеет место тогда и только тогда, когда  $x + y$  четно. Отсюда видно, что 2 имеет только один простой дивизор. Пусть  $\mu$  — кратность, с которой  $A$  делит 2. По основной теореме, 2 делит  $x + y \sqrt{D}$  тогда и только тогда, когда  $A^\mu$  делит  $x + y \sqrt{D}$ . Так как ни  $1 + \sqrt{D}$ , ни  $1 - \sqrt{D}$  не делится на 2,  $1 - D = (1 + \sqrt{D}) \times (1 - \sqrt{D})$  не может делиться на  $A^{2\mu}$ . С другой стороны,  $1 - D$  должно делиться на  $A^{2\mu}$ , поскольку на него делится  $2^2 = 4$ , а 4 делит  $1 - D$ . Это противоречие показывает, что в случае  $D \equiv 1 \pmod{4}$  построить теорию дивизоров для чисел вида  $x + y \sqrt{D}$  невозможно.

Бурбаки [ВЗ, стр. 127] придерживается мнения, что именно это очевидное противоречие помешало Куммеру развить теорию «идеальных комплексных чисел вида  $x + y \sqrt{D}$ ». Однако странно, что Куммеру удалось создать эту теорию как раз *только* в случае  $D \equiv 1 \pmod{4}$ . Например, при  $D = -3$  числа вида  $x + y \sqrt{D}$  содержатся среди круговых целых с  $\lambda = 3$ , поскольку в этом случае в качестве кубического корня  $\alpha$  из 1 можно взять  $\alpha = (-1 + \sqrt{-3})/2$ , так что  $x + y \sqrt{-3} = x + y + 2\alpha y$  — круговое целое. Вообще, как заметил Куммер (см. [К8, стр. 366] и [К11, стр. 114]), если  $D \equiv 1 \pmod{4}$  и  $|D|$  — простое число, скажем  $|D| = \lambda$ , то числа вида  $x + y \sqrt{D}$  содержатся среди круговых целых для этого  $\lambda$ , и теория дивизоров для таких чисел *следует* из теории дивизоров круговых целых (см. § 5.6).

Как же тогда разрешить обнаруженное выше противоречие? Если мы внимательно проследим за доказательством невозможности теории дивизоров при  $D = -3$ , то обнаружим, что оно ошибочно там, где утверждается, что 2 не делит  $1 - \sqrt{D}$ . Действительно, если числа вида  $x + y \sqrt{-3}$  рассматривать как подмножество круговых целых  $a + b\alpha$  ( $\alpha^3 = 1$ ), то 2 делит  $1 - \sqrt{-3}$  и частным является круговое целое  $-\alpha$ . Вообще, если мы утверждаем, что 2 *обязано* делить  $1 - \sqrt{D}$  при  $D \equiv 1 \pmod{4}$ , то отмеченное противоречие автоматически снимается и, как будет показано ниже, можно создать теорию дивизоров.

**Определение.** Если  $D$  — свободное от квадратов целое и  $D \not\equiv 1 \pmod{4}$ , то *квадратичным целым* детерминанта  $D$  называется число вида  $x + y\sqrt{D}$  при целых  $x$  и  $y$ . Если же  $D$  свободно от квадратов и  $D \equiv 1 \pmod{4}$ , то квадратичным целым детерминанта  $D$  называется число вида  $x + y \cdot (1 - \sqrt{D})/2$ , где  $x$  и  $y$  — целые числа. Иначе говоря, квадратичным целым детерминанта  $D \equiv 1 \pmod{4}$  называется число вида  $u + v\sqrt{D}$ , где  $u$  и  $v$  либо одновременно являются целыми, либо полуцелыми, т. е.  $2u$  и  $2v$  — нечетные целые. (Другое, более естественное, определение квадратичных целых детерминанта  $D$  можно найти в упр. 3).

Ясно, что множество определенных таким образом квадратичных целых замкнуто относительно операции сложения (сумма двух квадратичных целых является квадратичным целым), но не вполне очевидно, что при  $D \equiv 1 \pmod{4}$  оно замкнуто относительно умножения. Это следует из замечания, что при  $\omega = (1 - \sqrt{D})/2$  число  $\omega^2 = 1/4(1 + D) - 1/2\sqrt{D} = \omega + 1/4(D - 1)$  является квадратичным целым.

Приведенные выше определения простых дивизоров чисел  $p$  при простых  $p \neq 2$  и родственных понятий применимы и к квадратичным целым детерминанта  $D \equiv 1 \pmod{4}$ . Единственное отличие состоит в том, что  $x + y\sqrt{D}$  может быть числом с полуцелыми  $x$  и  $y$ . Нам остается только определить простые дивизоры числа 2 при  $D \equiv 1 \pmod{4}$ . Это можно сделать следующим образом.

Пусть  $A$  — простой дивизор числа 2. Поскольку каждое квадратичное целое можно записать в виде  $x + y\omega$  ( $\omega = (1 - \sqrt{D})/2$ ) и поскольку сравнения по модулю  $A$  для целых чисел совпадают со сравнениями по модулю 2, естественно спросить, сравнимо ли  $\omega$  с каким-либо целым по модулю  $A$ , т. е. делится ли  $\omega(\omega - 1)$  на  $A$ . Так как

$$\omega(\omega - 1) = 1/2(1 - \sqrt{D}) - 1/2(-1 - \sqrt{D}) = (D - 1)/4$$

является целым числом, то оно делится на  $A$  тогда и только тогда, когда оно четно; последнее справедливо в том и только в том случае, когда  $D \equiv 1 \pmod{8}$ . Таким образом, если  $D \equiv 1 \pmod{8}$ , то  $A$  делит либо  $\omega$ , либо  $\omega - 1$ . Дивизор  $A$  не может делить оба этих числа одновременно, поскольку тогда он делил бы  $1 = \omega - (\omega - 1)$ . Если  $A$  делит  $\omega$ , то сопряженный к нему дивизор делит  $\bar{\omega} = 1/2(1 + \sqrt{D}) = 1 - \omega$ , а если он делит  $\omega - 1$ , то сопряженный к нему делит  $\bar{\omega} - 1 = -\omega$ . В любом случае существуют два *различных* простых дивизора числа 2. Поскольку норма 2 равна  $2^2$ , мы получаем, что  $A\bar{A}$  является дивизором числа 2. Таким образом, дивизор 2 равен произведению двух простых дивизоров. Тот из них, который делит  $\omega$ , делит  $x + y\omega$  с крат-

ностью  $\mu$  тогда и только тогда, когда он делит  $(x + y\omega)(\omega - 1)^\mu$ , что справедливо в том и только в том случае, когда  $2^\mu$  делит  $(x + y\omega)(\omega - 1)^\mu$ . Аналогично, простой дивизор числа 2, который делит  $\omega - 1$ , делит  $x + y\omega$  с кратностью  $\mu$  тогда и только тогда, когда  $2^\mu$  делит  $(x + y\omega)\omega^\mu$ . В оставшемся случае, когда  $p = 2$ ,  $D \equiv 1 \pmod{4}$ ,  $D \not\equiv 1 \pmod{8}$ , т. е. когда  $D \equiv 5 \pmod{8}$ , то же самое рассуждение, что и выше, показывает, что  $\omega$  не сравнимо ни с каким целым по модулю  $A$  и, следовательно, согласно приведенному выше соображению, не существует квадратичного целого  $x + y\omega$ , которое делилось бы на  $A$ , но не делилось на 2. Таким образом, в этом случае следует ожидать, что делимость на  $A$  совпадает с делимостью на 2, т. е. что 2 является простым. Для того чтобы доказать это утверждение, необходимо и достаточно доказать, что 2 делит норму  $(x + y\omega)(x + y\bar{\omega})$  числа  $x + y\omega$  тогда и только тогда, когда 2 делит  $x + y\omega$  (упр. 1). Далее,  $(x + y\omega)(x + y\bar{\omega}) = x^2 + (\omega + \bar{\omega})xy + \omega\bar{\omega}y^2 = x^2 + xy - \frac{1}{4}(D - 1)y^2$ . Согласно предположению,  $\frac{1}{4}(D - 1)$  — нечетное целое, поэтому  $x^2 + xy - \frac{1}{4}(D - 1)y^2 \equiv x^2 + xy + y^2 \pmod{2}$  четно, только если  $x$  и  $y$  оба четны, т. е. 2 делит норму  $x + y\omega$  только в том случае, когда оно делит  $x + y\omega$ .

**Определение.** Если  $D \equiv 1 \pmod{8}$ , то 2 имеет два простых дивизора, один из которых делит  $x + y\omega$  с кратностью  $\mu$ , если  $2^\mu$  делит  $(x + y\omega)(\omega - 1)^\mu$ , а другой делит  $x + y\omega$  с кратностью  $\mu$ , если  $2^\mu$  делит  $(x + y\omega)\omega^\mu$ . (Здесь  $\omega = (1 - \sqrt{D})/2$ .) Если  $D \equiv 5 \pmod{8}$ , то единственным простым дивизором числа 2 является дивизор, определенный условием: « $A$  делит  $x + y\omega$  с кратностью  $\mu$ , если  $2^\mu$  делит  $x + y\omega$ ».

Это завершает анализ, т. е. поиски пути, на котором должны быть определены простые дивизоры. Синтез, т. е. доказательство того, что данные определения приводят к непротиворечивой теории, в которой имеют место ожидаемые свойства, будет проведен в следующем параграфе.

**Резюме.** Есть три различных способа, которыми данное простое положительное целое  $p$  может «разложиться на множители», если мы будем рассматривать его как квадратичное целое детерминанта  $D$ . Во-первых,  $p$  может *остаться простым*, т. е. дивизор  $p$  может быть простым дивизором. Во-вторых,  $p$  может *распадаться*, т. е. его дивизор может быть произведением двух различных простых дивизоров. Наконец, дивизор  $p$  может быть квадратом простого дивизора. В этом случае, по аналогии с теорией римановых поверхностей, говорят, что  $p$  *разветвляется*. Если  $p \neq 2$ , то  $p$  остается простым при  $D^{(p-1)/2} \equiv -1 \pmod{p}$ , распадается при  $D^{(p-1)/2} \equiv 1 \pmod{p}$  и разветвляется при  $D^{(p-1)/2} \equiv 0 \pmod{p}$ . Этот критерий можно выразить иначе, если сказать,



что  $p$  остается простым, когда сравнение  $u^2 \equiv D \pmod{p}$  не имеет решений, распадается, когда сравнение  $u^2 \equiv D \pmod{p}$  имеет два различных решения по модулю  $p$ , и разветвляется, когда сравнение  $u^2 \equiv D \pmod{p}$  имеет одно решение  $u \equiv 0 \pmod{p}$ . Простое 2 остается простым, если  $D \equiv 5 \pmod{8}$ , распадается, если  $D \equiv 1 \pmod{8}$ , и разветвляется, если  $D \equiv 2$  или  $3 \pmod{4}$ . (Поскольку  $D$  свободно от квадратов, случай  $D \equiv 0 \pmod{4}$  не рассматривается.)

**Обозначения.** В дальнейшем полезно иметь обозначения для простых дивизоров. Если  $p$  — простое целое, которое остается простым, его дивизор мы обозначим через  $(p)$ . Если  $p$  — разветвленное простое, то через  $(p, *)$  мы будем обозначать его единственный простой дивизор. Тогда  $(p, *)^2$  — дивизор  $p$ . Если  $p$  — распадающееся простое при  $p \neq 2$ , а  $u$  — решение сравнения  $u^2 \equiv D \pmod{p}$ , то через  $(p, u)$  обозначим простой дивизор  $p$ , который делит  $u - \sqrt{D}$ , т. е. простой дивизор  $p$ , по модулю которого  $\sqrt{D} \equiv u$ . Тогда  $(p, u)(p, -u)$  — дивизор  $p$ . Если 2 распадается (т. е. если  $D \equiv 1 \pmod{8}$ ), то через  $(2, 0)$  и  $(2, 1)$  мы будем обозначать простые дивизоры числа 2, по модулю которых  $(1 - \sqrt{D})/2 \equiv 0$  и  $1$  соответственно. В этом случае дивизор 2 равен  $(2, 0)(2, 1)$ . В противном случае 2 либо остается простым, либо разветвляется и имеет дивизор  $(2)$  или  $(2, *)^2$  соответственно.

## Упражнения

1. Докажите, что  $p$ , рассматриваемое как квадратичное целое детерминанта  $D$ , является простым тогда и только тогда, когда из  $p \mid (x^2 - Dy^2)$  следует, что  $p \mid (x + y\sqrt{D})$ .

2. Докажите, что если  $D \equiv 1 \pmod{4}$ , то норма  $x^2 - Dy^2$  любого квадратичного целого является *целым числом*.

3. Пусть  $a = x + y\sqrt{D}$ , где  $x$  и  $y$  — произвольные вещественные числа. Докажите, что  $a$  является квадратичным целым детерминанта  $D$  тогда и только тогда, когда многочлен второй степени  $(X - a)(X - \bar{a})$  имеет целые коэффициенты. Следовательно, квадратичным целым можно назвать произвольное число, удовлетворяющее уравнению вида  $X^2 + bX + c = 0$  с целыми  $b$  и  $c$ .

4. Покажите, что если  $p \mid D$ , то  $(p, *)$  делит  $x + y\sqrt{D}$  тогда и только тогда, когда  $x \equiv 0 \pmod{p}$ . Докажите также, что  $p$  делит  $x + y\sqrt{D}$  в том и только в том случае, когда  $(p, *)$  делит  $x + y\sqrt{D}$  с кратностью, не меньшей двух.

5. Перечислите все свободные от квадратов целые  $D$  с  $|D| \leq 10$ .

6. При  $D = -1$  воспользуйтесь теоремой Жирара о суммах двух квадратов (см. § 1.7), чтобы точно указать, какие простые  $p$  распадаются, какие разветвляются и какие остаются простыми.

7. Опишите, как разлагаются простые  $p$  (т. е. распадаются ли они, разветвляются или остаются простыми) при  $D = -2$ . (Воспользуйтесь теоремами из гл. 2 о числах вида  $x^2 + 2y^2$ .)

8. Опишите разложение простых  $p$  при  $D = 2$ .

9. Используя результаты о разложении простых в круговых целых при  $\lambda = 3$ , опишите разложение простых  $p$  для  $D = -3$ .

10. Используя круговые целые для  $\lambda = 5$ , опишите разложение простых при  $D = 5$ .

11. Используя метод проб и ошибок, найдите все простые, меньшие 20, которые распадаются при  $D = -5$ . Используйте квадратичный закон взаимности и решите эту задачу в общем виде.

12. Для каждого свободного от квадратов  $D$  с  $|D| \leq 5$  найдите все дивизоры с нормой 36.

13. Докажите, что если  $D \equiv 1 \pmod{4}$  и простое  $p$  распадается, то каждое квадратичное целое сравнимо с некоторым обыкновенным целым по модулю  $(p, u)$  (где  $(p, u)$  — один из простых дивизоров  $p$ ).

## 7.2. Теория дивизоров

Пусть квадратичные целые детерминанта  $D$  определены, как в предыдущем параграфе (т. е. при  $D \equiv 1 \pmod{4}$  допускаются знаменатели 2); допустим также, что простые дивизоры  $(p)$ ,  $(p, *)$ ,  $(p, u)$  определены аналогичным образом. Мы должны доказать, что эти определения дают непротиворечивую теорию дивизоров, обладающую ожидаемыми свойствами.

**Предложение 1.** *Если  $p$  остается простым, то  $p$  делится на один простой дивизор с кратностью точно 1 и не делится на другие простые дивизоры. Если  $p$  разветвляется, то  $p$  делится на один простой дивизор с кратностью точно 2 и не делится на другие простые дивизоры. Если  $p$  распадается, то  $p$  делится на два простых дивизора с кратностью точно 1 и не делится на другие простые дивизоры. Во всех случаях для деления на простое  $p$  основная теорема справедлива в том смысле, что если  $x + y \sqrt{D}$  делится на все простые дивизоры  $p$  с кратностью, не меньшей той, с которой они делят  $p$ , то  $x + y \sqrt{D}$  делится на  $p$ .*

**Доказательство.** Из определения легко следует, что каждый простой дивизор делит лишь единственное простое целое. Следовательно, рассматривая простые дивизоры, делящие  $p$ , можно игнорировать все дивизоры, за исключением тех, которые определены в связи с данным  $p$ . Если  $p$  остается простым, то делимость на  $(p)$  означает обычную делимость на  $p$ , и доказывать нечего. Если  $p$  разветвляется, то делимость  $x + y \sqrt{D}$  на  $(p, *)$  с кратностью  $\mu$  означает делимость  $(x + y \sqrt{D}) \tau^\mu$  на  $p^\mu$ , где  $\tau = \sqrt{D}$ , если  $p \mid D$ , и  $\tau = 1 + \sqrt{D}$ , если  $p = 2$  и  $D$  нечетно. Таким образом,  $p$  делится на  $(p, *)$  с кратностью 2 тогда и только тогда, когда  $\tau^2$  делится на  $p$ , что, как легко видеть, справедливо в обоих случаях. Оно делится на  $(p, *)$  с кратностью точно 2, если  $p$  не делит  $(\tau^2/p) \tau$ . Если  $\tau = \sqrt{D}$ , то это немедленно следует из того, что  $D$  свободно от квадратов. Если же  $\tau = 1 + \sqrt{D}$ , то мы получаем это утверждение, используя равенство  $(\tau^2/p) \tau =$

$= 1/2 [(1 + 3D) + (3 + D) \sqrt{D}]$ , так как в этом случае  $D \equiv 3 \pmod{4}$ . Если  $x + y \sqrt{D}$  делится на  $(p, *)$  с кратностью 2, то  $p$  делит  $(\tau^2/p) (x + y \sqrt{D})$ . При  $\tau = \sqrt{D}$  отсюда следует, что  $p$ , как и требуется, делит  $x + y \sqrt{D}$ , поскольку в этом случае  $\tau^2/p$  — целое, взаимно простое с  $p$ . Если  $\tau = 1 + \sqrt{D}$  (и, следовательно,  $p = 2$ ,  $D \equiv 3 \pmod{4}$ ), то тот же самый вывод следует из сравнения  $(\tau^2/p) (x + y \sqrt{D}) \equiv \sqrt{D} (x + y \sqrt{D}) \equiv y + x \sqrt{D} \pmod{2}$ , которое показывает, что  $x + y \sqrt{D}$  делится на  $(p, *)$  с кратностью 2 только тогда, когда  $y \equiv x \equiv 0 \pmod{2}$ . Наконец, предположим, что  $p$  распадается. Очевидно, что  $p$  делится на каждый из его простых дивизоров с кратностью 1. Такой простой дивизор делит  $x + y \sqrt{D}$  с кратностью  $\mu$  тогда и только тогда, когда  $p^\mu$  делит  $(x + y \sqrt{D}) \tau^\mu$ , где  $\tau = u - \sqrt{D}$  при  $p \neq 2$  ( $u^2 \equiv D \pmod{p}$ ) и  $\tau = \omega$  или  $\omega - 1$  при  $p = 2$  (и, следовательно,  $D \equiv 1 \pmod{8}$ ),  $\omega = 1/2 (1 - \sqrt{D})$ . Для того чтобы доказать, что такой простой дивизор делит  $p$  с кратностью точно 1, необходимо и достаточно доказать, что  $p$  не делит  $\tau^2$ . Если  $p \neq 2$ , то это следует из сравнения  $\tau^2 = u^2 + D - 2\sqrt{D} \equiv 2(D - \sqrt{D}) \not\equiv 0 \pmod{p}$ . Если же  $p = 2$ , то мы приходим к такому же заключению, используя сравнения  $\tau^2 = \omega^2 = 1/4 (D + 1 - 2\sqrt{D}) = 1/4 (D - 1) + \omega \equiv \omega \not\equiv 0 \pmod{2}$  или  $\tau^2 = (\omega - 1)^2 \equiv \omega^2 - 1 \equiv \omega - 1 \not\equiv 0 \pmod{2}$ . Остается только доказать, что если  $x + y \sqrt{D}$  делится на оба простых дивизора, делящих  $p$ , то  $x + y \sqrt{D}$  делится на  $p$ . При  $p \neq 2$  это следует из замечания, что если  $p$  делит как  $(x + y \sqrt{D}) (u - \sqrt{D})$ , так и  $(x + y \sqrt{D}) (-u - \sqrt{D})$ , то оно делит  $2u (x + y \sqrt{D})$  и  $2u$  взаимно просто с  $p$ . Если же  $p = 2$  и 2 делит как  $(x + y \sqrt{D}) \omega$ , так и  $(x + y \sqrt{D}) (\omega - 1)$ , то 2 делит  $x + y \sqrt{D}$ .

**Предложение 2.** Пусть  $A$  — простой дивизор. Если  $A$  делит  $x + y \sqrt{D}$  и  $r + s \sqrt{D}$  одновременно с кратностью  $\mu$ , то  $A$  делит также и  $(x + y \sqrt{D}) + (r + s \sqrt{D})$  с кратностью  $\mu$ . Если  $A$  делит  $x + y \sqrt{D}$  с кратностью точно  $\mu$  (т. е. делит с кратностью  $\mu$ , но не с кратностью  $\mu + 1$ ) и делит  $r + s \sqrt{D}$  с кратностью точно  $\nu$ , то  $A$  делит  $(x + y \sqrt{D}) (r + s \sqrt{D})$  с кратностью точно  $\mu + \nu$ . Наконец, если  $x + y \sqrt{D} \neq 0$ , то существует единственное целое  $\mu \geq 0$ , такое, что  $A$  делит  $x + y \sqrt{D}$  с кратностью точно  $\mu$ .

**Доказательство.** Первое из этих утверждений очевидно во всех случаях. Для доказательства второго утверждения полез-

но рассмотреть сначала случай  $\mu = \nu = 0$ , когда утверждается, что *простой дивизор является простым*, т. е. если  $A$  не делит ни один из сомножителей, то  $A$  не может делить произведение. Если  $A = (p)$ , где  $p$  остается простым, то это утверждение было доказано в предыдущем параграфе. Если  $A = (p, *)$ , где  $p$  разветвляется, или  $A = (p, u)$ , где  $p$  распадается, то каждое квадратичное целое сравнимо с некоторым обыкновенным целым по модулю  $A$ , а два целых сравнимы по модулю  $A$  тогда и только тогда, когда они сравнимы по модулю  $p$ . Таким образом, из сравнения  $(x + yu)(r + su) \equiv (x + y\sqrt{D})(r + s\sqrt{D}) \equiv 0 \pmod{A}$  следует, что  $x + yu$  или  $r + su \equiv 0 \pmod{p}$  и, значит,  $x + y\sqrt{D}$  или  $r + s\sqrt{D} \equiv 0 \pmod{A}$ . Заметим далее, что  $A$  делит  $x + y\sqrt{D}$  с кратностью точно  $\mu$  тогда и только тогда, когда  $p^\mu$  делит  $(x + y\sqrt{D})\tau^\mu$ , но полученное частное не делится на  $A$  (где  $\tau = 1$ , если  $A = (p)$ ,  $\tau = \sqrt{D}$ , если  $A$  делит  $D$ ,  $\tau = \sqrt{D} + 1$ , если  $A = (2, *)$  и  $D$  нечетно,  $\tau = u - \sqrt{D}$ , если  $A = (p, u)$ ,  $p \neq 2$ , и  $\tau = \omega$  или  $\omega - 1$ , если  $A = (2, 0)$  или  $(2, 1)$  соответственно). Это утверждение просто сводится к замечанию, что  $A$  делит  $(x + y\sqrt{D})\tau^\mu/p^\mu$  тогда и только тогда, когда  $p$  делит  $(x + y\sqrt{D})\tau^{\mu+1}/p^\mu$ , последнее же справедливо в том и только в том случае, когда  $p^{\mu+1}$  делит  $(x + y\sqrt{D})\tau^{\mu+1}$  (при условии, что  $p^\mu$  делит  $(x + y\sqrt{D})\tau^\mu$ ). Таким образом,  $A$  не делит ни  $(x + y\sqrt{D})\tau^\mu/p^\mu$ , ни  $(r + s\sqrt{D})\tau^\nu/p^\nu$ , поэтому, как было только что показано,  $A$  не делит  $(x + y\sqrt{D})(r + s\sqrt{D})\tau^{\mu+\nu}/p^{\mu+\nu}$ . Следовательно,  $A$  делит произведение с кратностью точно  $\mu + \nu$ , что и требовалось доказать.

Далее, если  $A$  делит  $x + y\sqrt{D}$  с кратностью точно  $\mu$  и с кратностью точно  $\mu + j$ , где  $j > 0$ , то  $(x + y\sqrt{D})\tau^\mu/p^\mu$  не делится на  $A$ , но после домножения на  $\tau^j$  будет делиться на  $p^j$ , а потому и на  $A$ . Очевидно, что это возможно только в тех случаях, когда  $A$  делит  $\tau$ , т. е. когда  $A = (p, *)$ . Но тогда  $\tau^2 = p\sigma$ , где  $\sigma$  не делится на  $A$  (поскольку, как было показано выше,  $p$  не делит  $\sigma\tau = (\tau^2/p)\tau$ ). Тогда  $j$  не может быть четным. Действительно, если  $j = 2k$ , то  $(x + y\sqrt{D})\tau^{\mu+j} = p^{\mu+k}[(x + y\sqrt{D})\tau^\mu/p^\mu]\sigma^k$  делится на  $p^{\mu+k}$ , но частное не делится на  $A$ , а потому и на  $p^k$ . Не может  $j$  быть и нечетным, так как если  $j = 2k + 1$  ( $k \geq 0$ ), то  $(x + y\sqrt{D})\tau^{\mu+j} = p^{\mu+k}[(x + y\sqrt{D})\tau^\mu/p^\mu]\sigma^k\tau$  только тогда делится на  $p^{\mu+k+1}$ , когда  $A$  делит  $[(x + y\sqrt{D})\tau^\mu/p^\mu]\sigma^k$ , что невозможно. Остается только доказать, что если  $x + y\sqrt{D} \neq 0$ , то  $x + y\sqrt{D}$  по крайней мере для одного  $\mu$  делится на  $A$  с кратностью точно  $\mu$ . Согласно определению, достаточно показать, что существует по крайней мере одно такое целое  $\nu > 0$ , что

$x + y \sqrt{D}$  не делится  $v$ -кратно на  $A$ . Для этого положим  $N(x + y \sqrt{D}) = p^n k$ , где  $k$  взаимно просто с  $p$ . Так как  $p$  самое бóльшее двукратно делится на  $A$ , а  $k$  вообще на него не делится, то  $p^n k$  не делится  $(2n + 1)$ -кратно на  $A$  и, следовательно,  $x + y \sqrt{D}$  тоже не делится  $(2n + 1)$ -кратно на  $A$ . Это завершает доказательство.

**Основная теорема.** Квадратичное целое  $x + y \sqrt{D}$  делит квадратичное целое  $u + v \sqrt{D}$  тогда и только тогда, когда каждый простой дивизор, делящий  $x + y \sqrt{D}$ , делит  $u + v \sqrt{D}$  с меньшей кратностью.

*Доказательство.* Это утверждение легко следует из предложений 1 и 2, если использовать рассуждения из § 4.11.

**Следствие.** Если два квадратичных целых делятся в точности на одни и те же простые дивизоры с одними и теми же кратностями, то их частное является единицей, т. е. квадратичным целым, которое делит 1.

*Доказательство.* Частное этих чисел не делится ни на один простой дивизор. Следовательно, согласно основной теореме, оно должно делить все квадратичные целые и, в частности, оно должно делить 1.

*Дивизором квадратичного целого* называется список всех простых дивизоров, которые делят это квадратичное целое, засчитанных с их кратностями. *Дивизор* есть (конечный) список простых дивизоров, в который некоторые простые дивизоры могут входить более одного раза. *Пустой дивизор*, который является дивизором числа 1, мы будем обозначать  $I$ . *Произведением* двух дивизоров называется список, полученный объединением списков дивизоров-сомножителей. Произведения мы будем записывать обычным образом, выписывая множители один за другим. Таким образом,  $(2, *)^2(3, 1)^2(17, 5)$  обозначает дивизор (для некоторого  $D$ , которое должно быть ясно из контекста), который содержит дважды дивизоры  $(2, *)$  и  $(3, 1)$  и один раз дивизор  $(17, 5)$ . При таких определениях задано отображение

$$\left\{ \begin{array}{l} \text{ненулевые} \\ \text{квадратичные} \\ \text{целые} \end{array} \right\} \rightarrow \{\text{дивизоры}\},$$

и оно обладает свойствами (ii)—(v) из § 4.15. (Доказательство свойства (iv) см. в упр. 4.)

Так же как в гл. 5 (и по тем же самым причинам), можно определить понятие *эквивалентности* дивизоров. Дивизор, который является дивизором квадратичного целого, называется *главным дивизором*. (О происхождении этой терминологии см. § 8.5.) Два дивизора  $A$  и  $B$  называются *эквивалентными* (что обозначается  $A \sim B$ ), если для любого дивизора  $C$  дивизор вида  $AC$  является главным тогда и только тогда, когда  $BC$  — главный дивизор. Другими словами, в любом дивизоре, делящемся на  $A$ ,  $A$  можно заменить на  $B$ , и новый дивизор будет главным в том и только в том случае, когда главным был исходный дивизор. Это отношение, очевидно, является рефлексивным, симметричным и транзитивным и оно согласовано с умножением дивизоров. Кроме того, справедливы все свойства (1) — (8) из § 5.3. Например,  $A$  является главным тогда и только тогда, когда  $A \sim I$ . Предложенное Куммером определение эквивалентности  $A \sim B$ , согласно которому должен существовать такой третий дивизор  $C$ , что дивизоры  $AC$  и  $BC$  являются главными, равносильно приведенному здесь определению.

Как и в случае круговых целых, можно найти конечную *систему представителей*, т. е. конечное множество дивизоров, обладающее тем свойством, что каждый дивизор эквивалентен в точности одному дивизору из этого множества. Мы докажем это утверждение в § 7.4; при этом мы получим конструктивный метод *построения* такого множества представителей. В круговом случае такое построение значительно сложнее, и мы даже не пытались найти его в гл. 5.

Каждый дивизор  $A$  имеет сопряженный к нему дивизор  $\bar{A}$ , определенный условием:  $A$  делит  $x + y \sqrt{D}$  с кратностью  $\mu$  тогда и только тогда, когда  $\bar{A}$  делит  $x - y \sqrt{D}$  с кратностью  $\mu$ . [Другими словами,  $\bar{A}$  получается из  $A$ , если в списке  $A$  мы оставим дивизоры  $(p)$  и  $(p, *)$  без изменения, а дивизоры  $(p, u)$  заменим на сопряженные к ним  $(p, -u)$  при  $p \neq 2$ , а при  $p = 2$ ,  $D \equiv \equiv 1 \pmod{8}$  сделаем замену  $(2, 0) \leftrightarrow (2, 1)$ .] Тогда естественно рассматривать дивизор  $A\bar{A}$  как *норму*  $A$ . Как и в круговом случае, часто бывает полезно рассматривать норму дивизора не как дивизор, а как обыкновенное *целое число*. Легко доказать, как и в круговом случае, что найдется единственное *положительное* целое число, дивизор которого равен  $A\bar{A}$ . Возникает искушение назвать его нормой  $A$ . Так естественно сделать при  $D < 0$ , поскольку в этом случае все нормы  $x^2 - Dy^2$  положительны. При  $D > 0$  нормы могут быть отрицательными, и норму дивизора следует определить иначе. Это является предметом следующего, очень короткого, параграфа.



## Упражнения

1. Докажите, что если  $AB$  — главный дивизор и  $A$  — главный дивизор, то  $B$  также является главным дивизором.

2. Найдите дивизоры следующих квадратичных целых (значением  $D$  в каждом случае является целое под знаком радикала):

- |                        |                          |
|------------------------|--------------------------|
| (a) $4 + 7\sqrt{3}$ ,  | (d) $\sqrt{21}$ ,        |
| (b) $5 - 9\sqrt{-2}$ , | (e) $55 + 12\sqrt{21}$ , |
| (c) $3\sqrt{-5}$ ,     | (f) $20 + 5\sqrt{14}$ .  |

3. Докажите, что дивизор произведения двух квадратичных целых равен произведению их дивизоров.

4. Докажите, что если  $A$  и  $B$  — дивизоры и если каждое квадратичное целое, делящееся на  $A$ , делится также и на  $B$ , то  $A$  делится на  $B$ . [За образец возьмите доказательство теоремы из § 4.13.]

## 7.3. Знак нормы

В теории дивизоров круговых целых было полезно считать нормой дивизора положительное целое, дивизор которого равен произведению всех дивизоров, сопряженных к данному. Тогда среди прочих полезных свойств получался тот факт, что если дивизор является главным и равен дивизору кругового целого  $f(\alpha)$ , то его норма равна  $Nf(\alpha)$ . (Действительно, в терминологии Куммера нет различия между обыкновенным целым  $Nf(\alpha)$  и идеальным комплексным числом  $Nf(\alpha)$ .) Если  $D < 0$ , то нормы  $x^2 - Dy^2$  всегда положительны, и норму дивизора  $A$  можно определить для квадратичных целых аналогичным образом, а именно:  $N(A)$  равна положительному целому с дивизором  $A\bar{A}$ . Однако при  $D > 0$  это определение неудовлетворительно, поскольку в этом случае норма дивизора квадратичного целого не всегда будет совпадать с нормой самого квадратичного целого.

От этой аномалии можно избавиться, введя при  $D > 0$  некоторый новый дивизор, норма которого равна  $-1$ . Поскольку в этом случае должен быть ровно один такой дивизор, он сопряжен самому себе и его естественно обозначить  $(-1, *)$ . Тогда *дивизор квадратичного целого*, который является списком всех простых дивизоров, делящих данное квадратичное целое, с учетом их кратностей, следует изменить таким образом, чтобы он *включал*  $(-1, *)$ , *если норма этого целого отрицательна, и не включал*  $(-1, *)$  *в противном случае*. Для того чтобы дивизор произведения был произведением дивизоров, необходимо и достаточно по определению считать  $(-1, *)^2 = I$ . При таких определениях выполняются все обычные свойства. (Из  $(-1, *)^2 = I$  следует, что  $(-1, *)$  делит любое квадратичное целое; таким образом, этот дивизор не удовлетворяет условиям основной теоремы.) Кроме того, норма дивизи-

зора является целым со знаком, которое в случае главного дивизора совпадает с нормой соответствующего квадратичного целого.

Дивизор  $(-1, *)$  является главным тогда и только тогда, когда существует квадратичное целое с нормой  $-1$ . Как показывают примеры (см. упражнения), в зависимости от данного  $D > 0$  дивизор  $(-1, *)$  может быть главным, а может и не быть.

В дальнейшем при  $D > 0$  в число дивизоров мы всегда будем включать дивизор  $(-1, *)$  (при  $D < 0$  этот дивизор никогда не рассматривается). Следует специально отметить, что при  $D > 0$  *утверждение, согласно которому любой дивизор однозначно определяется множеством всех делящихся на него квадратичных целых, другими словами, свойство (iv) из § 4.15 не является более справедливым*, если в число дивизоров мы включаем  $(-1, *)$ . Действительно, любое квадратичное целое делится как на  $I$ , так и на  $(-1, *)$ , но  $(-1, *) \neq I$ . Вообще  $(-1, *)$   $A$  делит те же самые квадратичные целые, что и  $A$ . Теорема из § 4.13 остается справедливой в новой теории, но ее следствие неверно, так как из  $A \mid B$  и  $B \mid A$  больше не вытекает, что  $A = B$ ; в этом случае выполняется лишь либо  $A = B$ , либо  $A = (-1, *) B$ .

В § 4.13 мы указали, что Дедекинды отождествлял идеальное комплексное число с множеством всех делящихся на него объектов. Множество, состоящее из всех таких элементов, Дедекинды назвал идеалом (что в этих случаях совпадает с дивизором). Из приведенного выше замечания следует, что, *с точки зрения Дедекинды,  $A$  и  $(-1, *) A$  неразличимы*, и действительно, в большинстве современных изложений такое различие не делается. Тем не менее такое различие полезно, и Гаусс неизменно его проводил (правда, в другом контексте). В этой книге мы будем различать дивизоры  $A$  и  $(-1, *) A$  не только потому, что это выглядит естественным, но и потому, что легче игнорировать различие там, где оно несущественно, чем вводить его после того, как вся теория развита без него. Кроме того, оказывается, что такое различие существенно для гауссова доказательства квадратичного закона взаимности в § 7.11.

## Упражнения

1. Найдите квадратичное целое детерминанта  $D = 2$  с дивизором  $(-1, *)$ . Найдите его квадрат и куб и их дивизоры.
2. Докажите, что дивизор  $(-1, *)$  не является главным при  $D = 3$ .
3. Докажите, что при  $D = 5$  дивизор  $(-1, *)$  главный.
4. Докажите теорему из § 4.13 для теории с дивизором  $(-1, *)$ .

## 7.4. Квадратичные целые с данными дивизорами

Однозначность разложения имеет место для дивизоров согласно самому их определению — всякий дивизор *есть* произведение простых дивизоров. Основная теорема показывает, что разложе-

ние квадратичного целого влечет за собой разложение его дивизора. Все разложения дивизора легко перечислить, поэтому задача разложения квадратичного целого приводит к задаче определения для данного дивизора, является ли он дивизором квадратичного целого, и, если это так, нахождения всех квадратичных целых, дивизором которых он является. Этот параграф, как указывает его название, посвящен решению данной задачи.

Пусть  $A$  — заданный дивизор. Прежде всего мы должны установить, является ли  $A$  главным, т. е. верно ли, что  $A \sim I$ . Естественный подход к этой задаче (который в точности совпадает с подходом, использованным в § 4.4 и § 4.7 при нахождении круговых целых с заданными дивизорами) заключается в попытке найти *делящиеся* на  $A$  квадратичные целые  $x + y \sqrt{D}$  с малыми в некотором смысле  $x$  и  $y$ . Для этого естественно попытаться найти простой способ проверки, делится ли данное квадратичное целое на  $A$ .

Заметим прежде всего, что если  $A$  делится на целое  $n$ , или, точнее, если  $A$  делится на дивизор  $(n)$  целого числа  $n$ , скажем  $A = (n) A'$ , то деление на  $n$  задает взаимно однозначное соответствие между квадратичными целыми с дивизором  $A$  (если такие найдутся) и квадратичными целыми с дивизором  $A'$ . Следовательно, не ограничивая общности, мы можем свести задачу к случаю, когда данный дивизор  $A$  не делится на дивизор ни одного целого, большего 1.

*Если  $A$  не делится ни на одно целое, большее 1, то каждое квадратичное целое сравнимо по модулю  $A$  с некоторым обыкновенным целым, и два квадратичных целых сравнимы по модулю  $A$  тогда и только тогда, когда они сравнимы по модулю нормы  $A$ . Это утверждение можно доказать следующим образом. Поскольку  $A$  не делится на  $(p)$ , или на  $(p, *)^2$ , или на  $(p, u) (p, -u)$  (где  $p$  соответственно остается простым, разветвляется или распадается<sup>1)</sup>), то он должен иметь вид*

$$A = (p_1, u_1)^{\mu_1} (p_2, u_2)^{\mu_2} \dots (p_\sigma, u_\sigma)^{\mu_\sigma} (p'_1, *) (p'_2, *) \dots (p'_\tau, *),$$

где  $p_1, p_2, \dots, p_\sigma$  — различные распадающиеся простые, причем  $\mu_1 \geq 1, \mu_2 \geq 1, \dots, \mu_\sigma \geq 1$ , и где  $p'_1, p'_2, \dots, p'_\tau$  — различные разветвленные простые. (Конечно,  $\sigma$  или  $\tau$  может быть равно 0.) Если  $D > 0$ , то  $p'_i$  при некотором  $i$  могло бы быть равно  $-1$ . Однако в этом случае  $A' = (-1, *) A$  не содержит дивизор  $(-1, *)$ , и, поскольку сравнения по модулю  $A$  совпадают со сравнениями по модулю  $A'$ , достаточно доказать нашу теорему для  $A'$ . Другими словами, не ограничивая общности, можно считать, что  $p'_i \neq -1$  при  $i = 1, 2, \dots, \tau$ . Норма  $A$  равна  $p_1^{\mu_1} p_2^{\mu_2} \dots$

<sup>1)</sup> Если 2 распадается, т. е. если  $D \equiv 1 \pmod{8}$ , то  $(p, u) (p, -u)$  здесь означает  $(2, 0) (2, 1)$ .

$\dots p_{\sigma}^{\mu_{\sigma}} p_1' p_2' \dots p_{\tau}'$ . Это целое мы обозначим через  $a$ . Если некоторое целое делится на  $A$ , то оно делится и на  $\bar{A}$  — это видно непосредственно из определения. Для множителей вида  $(p, u)^{\mu}$  дивизора  $A$  отсюда следует, что данное целое делится на  $(p, u)^{\mu} (p, -u)^{\mu}$ , а потому оно делится и на  $p^{\mu}$ . С другой стороны, простой дивизор вида  $(p, *)$  делит какое-либо целое только тогда, когда  $p$  делит это целое. Поскольку все  $p_i$  и  $p_i'$  различны, отсюда следует, что целое делится на  $A$  тогда и только тогда, когда оно делится на  $a$ . Остается доказать, что каждое квадратичное целое сравнимо с некоторым обыкновенным целым по модулю  $A$ .

Сначала рассмотрим случай  $D \equiv 2$  или  $3 \pmod{4}$ . Тогда каждое квадратичное целое имеет вид  $x + y \sqrt{D}$  при целых  $x$  и  $y$ , и достаточно доказать существование такого целого  $r$ , что  $\sqrt{D} \equiv r \pmod{A}$ . Для каждого множителя  $(p, u)^{\mu}$  дивизора  $A$  найдется целое, а именно  $u$ , такое, что  $u \equiv \sqrt{D} \pmod{(p, u)}$ . Тогда  $(u - \sqrt{D})^{\mu} \equiv 0 \pmod{(p, u)^{\mu}}$ . Положим  $(u - \sqrt{D})^{\mu} = b + c \sqrt{D}$ . Целое  $c$  не делится на  $p$ , поскольку в противном случае выполнялись бы сравнения  $c \sqrt{D} \equiv 0 \pmod{(p, u)}$ ,  $b \equiv 0 \pmod{(p, u)}$ ,  $b \equiv 0 \pmod{p}$ ,  $b + c \sqrt{D} \equiv 0 \pmod{p}$ ,  $b + c \sqrt{D} \equiv 0 \pmod{(p, -u)}$ ,  $u - \sqrt{D} \equiv 0 \pmod{(p, -u)}$ , но  $u - \sqrt{D} \not\equiv 0 \pmod{(p, -u)}$ . Поэтому  $c$  и  $p^{\mu}$  взаимно просты и существует такое целое  $d$ , что  $cd \equiv 1 \pmod{p^{\mu}}$ . Отсюда следует, что  $db + dc \sqrt{D} \equiv db + \sqrt{D} \pmod{(p, u)^{\mu}}$ ,  $\sqrt{D} \equiv -db \pmod{(p, u)^{\mu}}$ . Таким образом,  $\sqrt{D}$  сравним по модулю  $(p, u)^{\mu}$  с некоторым целым числом. Аналогично,  $\sqrt{D} \equiv$  целое  $\pmod{(p', *)}$ , а именно:  $\sqrt{D} \equiv 0 \pmod{(p', *)}$  во всех случаях, кроме  $p = 2$ ,  $D \equiv 3 \pmod{4}$ ; в последнем случае  $\sqrt{D} \equiv 1 \pmod{(p, *)}$ . Таким образом, для каждого множителя  $(p, u)^{\mu}$  или  $(p', *)$  дивизора  $A$  найдется такое целое  $r_i$ , что  $\sqrt{D} \equiv r_i \pmod{(p, u)^{\mu}}$  или  $\pmod{(p', *)}$  тогда и только тогда, когда  $r \equiv r_i \pmod{p^{\mu}}$  или  $\pmod{p'}$ . Согласно китайской теореме об остатках, существует целое  $r$ , которое удовлетворяет всем этим сравнениям, следовательно,  $\sqrt{D} \equiv r \pmod{A}$ .

Если  $D \equiv 1 \pmod{4}$ , то каждое квадратичное целое имеет вид  $x + y\omega$  с целыми  $x$ ,  $y$  и  $\omega = (1 - \sqrt{D})/2$ . Поэтому достаточно доказать, что  $\omega$  сравнимо с некоторым целым по модулю  $A$ . Для множителей дивизора  $A$ , имеющих вид  $(p, u)^{\mu}$  или  $(p', *)$  с  $p \neq 2$ , приведенное выше рассуждение показывает, что  $\sqrt{D} \equiv r_i$  при некотором целом  $r_i$ . Тогда  $2\omega = 1 - \sqrt{D} \equiv 1 - r_i$ , и, обращая 2 по модулю  $p^{\mu}$  или по модулю  $p'$ , мы получаем целое, сравнимое с  $\omega$  по модулю  $(p, u)^{\mu}$  или по модулю  $(p', *)$ . Если  $p = 2$ , то  $D \equiv 1 \pmod{8}$  и соответствующий множитель дивизора  $A$  равен либо  $(2, 0)^{\mu}$ , либо  $(2, 1)^{\mu}$ . По определению,  $\omega \equiv 0$  или

$1 \pmod{(2, 0)}$  или  $\pmod{(2, 1)}$  соответственно. Тогда  $\omega^\mu$  или  $(1 - \omega)^\mu$  делится на  $(2, 0)^\mu$  или на  $(2, 1)^\mu$  и имеет вид  $b + c\omega$  при нечетном  $c$ . Действительно, в противном случае 2 делило бы  $\omega$  или  $1 - \omega$ . Таким образом,  $c$  обратимо по модулю  $2^\mu$ , и существует целое, сравнимое с  $\omega$  по модулю  $(2, 0)^\mu$  или по модулю  $(2, 1)^\mu$ . Теперь китайская теорема об остатках дает нам требуемое целое, сравнимое с  $\omega$  по модулю  $A$ .

Таким образом, если данный дивизор  $A$  не делится ни на одно целое, большее 1, то мы можем найти такое целое  $r$ , что  $r - \sqrt{D}$  делится на  $A$ . Кроме того,  $r$  можно привести по модулю  $a$ , где  $a$  — норма  $A$ . Этих замечаний достаточно для доказательства того, что *число классов конечно*, т. е. существует конечное множество дивизоров, обладающее тем свойством, что каждый дивизор эквивалентен некоторому элементу этого множества. Действительно, дивизор  $r - \sqrt{D}$  имеет вид  $AB$ , где норма  $b$  дивизора  $B$  удовлетворяет неравенству  $|ab| = |(r - \sqrt{D})(r + \sqrt{D})| \leq r^2 + |D| \leq \frac{1}{4}a^2 + |D|$ . Таким образом,  $|b| < |a|$ , если только не выполняются неравенства  $\frac{1}{4}a^2 + |D| \geq |ab| \geq a^2$ ,  $|D| \geq 3a^2/4$ ,  $|a| \leq 2\sqrt{|D|/3}$ . Далее,  $AB$  и  $\bar{B}B$  — главные дивизоры, поэтому  $A \sim \bar{B}$ . Норма  $\bar{B}$  равна  $b$  и меньше  $a$  по абсолютной величине, если  $|a| > 2\sqrt{|D|/3}$ . Если бы исходный дивизор  $A$  делился на какое-либо целое, большее 1, то его можно было бы заменить на эквивалентный дивизор с меньшей нормой, который не делится ни на одно целое, большее 1. Таким образом, *если норма дивизора  $A$  больше  $2\sqrt{|D|/3}$  по абсолютной величине, то он эквивалентен некоторому дивизору с меньшей по абсолютной величине нормой*. Согласно принципу бесконечного спуска, повторяя при необходимости такую редукцию, мы можем найти дивизор, который эквивалентен  $A$  и имеет норму  $|a| \leq 2\sqrt{|D|/3}$ . Это доказывает конечность числа классов, так как число дивизоров с нормой, меньшей данной границы, конечно.

Для установления, является ли данный дивизор главным, необходимо лишь незначительное уточнение этого процесса приведения. Рассмотрим сначала случай, когда  $D < 0$  и  $D \equiv 2$  или  $3 \pmod{4}$ . Пусть  $A_0$  — заданный дивизор; не ограничивая общности, можно считать, что  $A_0$  не делится ни на одно целое, большее 1. Тогда приведенная выше редукция дает  $A_0 \sim A_1$ , где  $A_0\bar{A}_1$  — дивизор  $r_0 - \sqrt{D}$ ,  $r_0$  — целое, сравнимое с  $\sqrt{D}$  по модулю  $A_0$ , и  $r_0$  приведено <sup>1)</sup> по модулю нормы  $a_0$  дивизора  $A_0$ . Так

<sup>1)</sup> Приведение состоит в том, чтобы сделать  $|r_0|$  возможно меньшим, так что  $-\frac{1}{2}a_0 \leq r_0 \leq \frac{1}{2}a_0$ . Могут оказаться возможными два значения:  $r_0 = -\frac{1}{2}a_0$  и  $r_0 = \frac{1}{2}a_0$ . Для определенности в таком случае мы будем выбирать положительное значение  $r_0 = \frac{1}{2}a_0$ .



как  $A_1$  делит  $r_0 + \sqrt{D}$ , а  $r_0 + \sqrt{D}$  не делится ни на одно целое, то и  $A_1$  не делится ни на одно целое. Следовательно, этот процесс можно повторить и получить последовательность эквивалентных дивизоров  $A_0 \sim A_1 \sim A_2 \sim \dots$ . Кроме того, как только заданы значения  $a_0$  и  $r_0$ , сразу же известно  $a_1 = (r_0^2 - D)/a_0$  и легко найти значение  $r_1$ . Действительно,  $A_1$  делит  $(-r_0) - \sqrt{D}$ , поэтому  $r_1$  равно  $-r_0$ , приведенному по модулю  $a_1$ . Аналогично, если известны  $a_i, r_i$ , то  $a_{i+1}, r_{i+1}$  можно найти из соотношений  $a_{i+1} = (r_i^2 - D)/a_i$  и  $r_{i+1} + r_i \equiv 0 \pmod{a_{i+1}}$ . Если существует такое  $i$ , что  $a_i = 1$ , то  $A_i = I$  и, в частности,  $A_i$  — главный дивизор. Таким образом, для того чтобы данный дивизор был главным, достаточно, чтобы последовательность целых чисел  $a_0, a_1, a_2, \dots$  содержала 1.

Теперь мы покажем, что это условие является также и *необходимым* (по-прежнему в предположениях  $D < 0$ ,  $D \equiv 2$  или  $3 \pmod{4}$ ). Согласно принципу бесконечного спуска, должно существовать такое  $i$ , что  $a_{i+1} \geq a_i$ , а отсюда, как было показано выше, следует, что  $a_i \leq 2\sqrt{|D|}/3$ . Значит,  $a_i \leq |D|$ , причем неравенство является строгим при  $D \neq -1$  ( $|D| \leq 2\sqrt{|D|}/3$  влечет за собой  $3|D|^2 \leq 4|D|$ ,  $|D| \leq 4/3$ ). Если  $A_0 \sim I$ , то  $A_i \sim I$  и существует квадратичное целое  $u + v\sqrt{D}$  с дивизором  $A_i$ . Тогда  $u^2 - Dv^2 = a_i \leq |D|$  со строгим неравенством при  $D \neq -1$ . Таким образом, если  $v \neq 0$ , то  $D = -1$ . Отсюда следует, что  $a_i \leq 1$ , т. е.  $a_i = 1$ , что и требовалось доказать. В противном случае  $v = 0$  и  $A_i$  — дивизор  $u$ , вопреки тому что  $A_i$  не делится ни на одно целое, большее 1 (за исключением того случая, когда  $u = \pm 1$  и  $a_i = 1$ ). Следовательно, из эквивалентности  $A_0 \sim I$  мы получаем не только то, что  $a_i = 1$  достигается, но также и то, что последовательность  $a_i$  убывает до тех пор, пока не достигнет  $a_i = 1$ .

Это дает нам очень простой алгоритм для определения (при  $D < 0$ ,  $D \equiv 2$  или  $3 \pmod{4}$ ), является ли данный дивизор главным. Лишь незначительное расширение этого алгоритма требуется для нахождения всех квадратичных целых с дивизором  $A$  при  $A \sim I$ . Пусть  $A \sim A_0 \sim A_1 \sim \dots \sim A_i = I$ , где  $A = (n)A_0$  и где  $A_j \bar{A}_{j+1}$  — дивизор целого  $r_j - \sqrt{D}$  при  $j = 0, 1, \dots, i-1$ . Если нам дано квадратичное целое с дивизором  $A_{j+1}$ , то мы можем найти квадратичное целое с дивизором  $A_j$ , умножив целое с дивизором  $A_{j+1}$  на  $r_j - \sqrt{D}$ , имеющее дивизор  $A_j \bar{A}_{j+1}$ , и разделив на  $a_{j+1}$  с дивизором  $A_{j+1} \bar{A}_{j+1}$ . Если мы начнем этот процесс с 1, имеющей дивизор  $I$ , то композиция этих операций даст нам квадратичное целое с дивизором  $A_0$ ; умножая затем на  $n$ , мы получим квадратичное целое с дивизором  $A$ . Согласно основной теореме, мы получим квадратичное целое с дивизором  $A$  в общем виде,



если умножим уже найденное квадратичное целое с дивизором  $A$  на единицу. Далее, единица  $u + v \sqrt{D}$  удовлетворяет соотношению  $u^2 - Dv^2 = \pm 1$ , поэтому или  $u = \pm 1, v = 0$  или  $D = -1$  и  $u = 0, v = \pm 1$ , т. е.  $\pm 1$  являются единственными единицами, за исключением случая  $D = -1$ , когда имеется 4 единицы:  $\pm 1, \pm \sqrt{-1}$ . Это завершает решение данной задачи в случае  $D < 0, D \equiv 2$  или  $3 \pmod{4}$ : за конечное число простых шагов мы можем определить, является ли данный дивизор главным, и, если это так, найти все квадратичные целые (их будет ровно два или, при  $D = -1$ , четыре) с данным дивизором.

В случае  $D < 0, D \equiv 1 \pmod{4}$  требуются лишь незначительные изменения. Если  $A$  задано, положим  $A = (n) A_0$ , где  $A_0$  не делится ни на одно целое, большее 1. Существует такое полуцелое (половина нечетного целого)  $r$ , что  $r - \frac{1}{2} \sqrt{D} \equiv 0 \pmod{A_0}$ . Пусть  $a_0$  — норма  $A_0$  и  $r_0$  — полуцелое, полученное приведением<sup>1)</sup>  $r$  по модулю  $a_0$ ; пусть  $A_1$  — такой дивизор, что  $A_0 \bar{A}_1$  является дивизором  $r_0 - \frac{1}{2} \sqrt{D}$ . Если  $a_1$  — норма  $A_1$ , то  $a_0 a_1 = r_0^2 - \frac{1}{4} D \leq \frac{1}{4} a_0^2 - \frac{1}{4} D$ . Если  $a_0$  не превосходит  $a_1$ , то  $a_0^2 \leq a_0 a_1 \leq (a_0^2 - D)/4, a_0 \leq \sqrt{|D|}/3$ . Следовательно, повторение этой процедуры приводит в конце концов к дивизору  $A_i$  с нормой  $a_i \leq \sqrt{|D|}/3$ . Это доказывает конечность числа классов. Если в последовательности  $a_0, a_1, a_2, \dots$  содержится значение 1, то  $A_i = I$ , и отсюда не только следует, что дивизор  $A$  является главным, но также и то, что мы можем найти все квадратичные целые с дивизором  $A$ , как только найдем все единицы. Если  $u^2 - Dv^2 = 1$  и  $u + v \sqrt{D} \neq \pm 1$ , то либо  $u = 0$ , либо  $u = \pm 1/2, -Dv^2 = 3/4, v = \pm 1/2, D = -3$ . Но равенство  $u = 0$  невозможно, поскольку тогда  $v$  является целым числом,  $-D < +1, D \geq -1$ , что противоречит предположению. Короче говоря, при  $D \neq -3$  единственными единицами являются  $\pm 1$ ; если же  $D = -3$ , то имеется шесть единиц  $\pm 1, \pm \frac{1}{2} \pm \frac{1}{2} \sqrt{-3}$ .

Теперь решение нашей задачи будет полным, если доказать, что в случае  $A \sim I$  последовательность  $a_0, a_1, a_2, \dots$  должна содержать значение 1. Пусть  $i$  — первое целое, для которого  $a_i \leq a_{i+1}$ . Тогда, как было показано выше,  $a_i \leq \sqrt{|D|}/3$ . Если  $A$  — главный дивизор, то существует квадратичное целое  $u + v \sqrt{D}$  с дивизором  $A_i$ . Тогда  $u^2 - Dv^2 = a_i \leq \sqrt{|D|}/3$ . Таким образом,  $\frac{1}{4} [(2u)^2 - D(2v)^2] \leq \sqrt{|D|}/3$  и  $2u, 2v$  — целые

<sup>1)</sup> В ситуации, когда это приведение неоднозначно, т. е. когда  $r \equiv \frac{1}{2} a_0 \pmod{a_0}$ , мы снова будем использовать положительное значение  $r_0 = \frac{1}{2} a_0$ .

числа. Если  $v \neq 0$ , то отсюда следует, что  $1/4(-D) \leq \sqrt{|D|/3}$ ,  $D^2 \leq 16|D|/3$ ,  $|D| \leq 6$ ,  $D = -3$ . Таким образом, если  $D \neq -3$ , то  $v = 0$ ,  $u$  — целое с дивизором  $A_i$ , и, поскольку  $A_i$  не делится ни на одно целое, большее 1,  $u = \pm 1$ ,  $A_i = I$ , что и требовалось доказать. Если же  $D = -3$ , то  $a_i \leq \sqrt{|D|/3} = 1$  и  $u + v\sqrt{D}$  должно быть единицей; отсюда снова следует, что  $A_i = I$ .

Теперь мы рассмотрим случай  $D > 0$  и для простоты предположим, что  $D \equiv 2$  или  $3 \pmod{4}$ . Рассуждение, при помощи которого мы доказывали конечность числа классов, проходит и в этом случае; оно показывает, что каждый дивизор эквивалентен дивизору с нормой, не превышающей  $2\sqrt{D/3}$  по абсолютной величине. Кроме того, это доказательство использует явную последовательность эквивалентных дивизоров  $A \sim A_0 \sim A_1 \sim \dots \sim A_i$ , в которой  $|N(A_i)| \leq 2\sqrt{D/3}$ . Поэтому мы получим решение нашей задачи для  $A$ , если сможем решить ее для  $A_i$ . Следовательно, не ограничивая общности, можно считать, что  $A = A_0$  не делится ни на одно целое, большее 1, и что  $|N(A)| \leq 2\sqrt{D/3}$ .

Пусть  $a_0$  — норма  $A_0$  и  $\sqrt{D} \equiv r_0 \pmod{A_0}$ ; предположим, что  $|a_0| \leq 2\sqrt{D/3}$ . Описанный выше процесс использует приведение  $r_0$  по модулю  $a_0$ , для того чтобы получить  $r_0$  с  $|r_0| \leq |a_0|/2$ . Однако наша главная цель состоит в том, чтобы сделать  $a_0a_1 = r_0^2 - D$  возможно меньшим по абсолютной величине; этой цели легче добиться, если приближать  $r_0$  к  $\pm\sqrt{D}$ , а не к 0. Возможно, читатель уже заметил, что использованные в этом процессе шаги очень похожи на шаги циклического метода из § 1.9. В циклическом методе оказалось эффективным выбирать в качестве  $r$  *положительное* число с возможно меньшим  $|r^2 - D|$ , но при доказательстве того, что циклический метод всегда дает все решения уравнения Пелля (см. упр. 9—13 к § 1.9), мы обнаружили, что удобнее выбирать  $r$  как можно большим, но таким, чтобы  $r^2 - D$  было *отрицательным*. Здесь мы будем применять тот же метод выбора  $r$ . Пусть  $r_0$  — наибольшее целое,  $r_0 \equiv \sqrt{D} \pmod{A_0}$ , для которого  $r_0^2 - D < 0$ . (Существует по меньшей мере одно  $r$ , удовлетворяющее соотношениям  $r \equiv \sqrt{D} \pmod{A_0}$  и  $r^2 - D < 0$ ; действительно, расстояние между корнями  $x^2 - D$  равно  $2\sqrt{D} \geq |a_0|\sqrt{3} > |a_0|$ .) Теперь, как и раньше, через  $A_1$  обозначим дивизор, определенный условием:  $A_0\bar{A}_1$  — дивизор  $r_0 - \sqrt{D}$ . Тогда норма  $A_1$  равна  $(r_0^2 - D)/a_0$  и  $\sqrt{D} \equiv -r_0 \pmod{A_1}$ . На следующем шаге в качестве  $r_1$  возьмем наибольшее целое  $r_1 \equiv \sqrt{D} \pmod{A_1}$ , для которого  $r_1^2 - D < 0$ , т. е. наибольшее целое, удовлетворяющее сравнению  $r_0 + r_1 \equiv 0 \pmod{a_1}$ , для которого  $r_1^2 - D < 0$ . Заметим, что такое  $r_1$  найдется всегда:

поскольку  $(-r_0)^2 - D < 0$ , в качестве  $r_1$  можно при необходимости выбрать  $-r_0$ .

Это правило выбора  $r_1$ , а впоследствии и  $r_2, r_3, \dots$ , определяет бесконечную последовательность дивизоров  $A_0 \sim A_1 \sim \dots \sim A_2 \sim \dots$ , эквивалентных  $A_0$ . Если последовательность  $a_0, a_1, a_2, \dots$  норм этих дивизоров содержит 1, то  $A_i = I$  для некоторого  $i$  и  $A_0$  — главный дивизор. Главная теорема состоит в том, что *это достаточное условие в действительности является и необходимым*, т. е. если  $A_0 \sim I$ , то определенная выше последовательность  $A_0 \sim A_1 \sim A_2 \sim \dots$  должна достигнуть  $A_i = I$ . Эта теорема будет доказана в следующем параграфе.

Легко доказать также (и это мы тоже сделаем в следующем параграфе), что последовательность  $A_0 \sim A_1 \sim A_2 \sim \dots$  в конце концов становится повторяющейся. Следовательно, при проверке, является ли данный дивизор  $A_0$  главным, нам надо продолжить последовательность  $A_0 \sim A_1 \sim A_2 \sim \dots$  только до того момента, с которого она начнет повторяться. Если к тому времени не встретится  $A_i = I$ , то такое  $A_i$  никогда не встретится и в этом случае, согласно теореме, которую мы докажем,  $A_0$  не является главным дивизором.

Если нам дано квадратичное целое с дивизором  $A_j$ , то, как и выше, мы найдем квадратичное целое с дивизором  $A_{j-1}$ , умножив данное целое на  $r_{j-1} - \sqrt{D}$  и разделив на  $a_j$ . Таким образом, если  $A_0 \sim I$ , то можно найти последовательность  $A_0 \sim A_1 \sim \dots \sim A_i = I$  и, начиная с квадратичного целого 1 с дивизором  $A_i$ , вернуться назад и найти квадратичное целое с дивизором  $A_0$ . Тогда самое общее квадратичное целое с дивизором  $A_0$  представляет собой произведение полученного выше квадратичного целого на единицу. Таким образом, полное решение нашей задачи сводится к нахождению самого общего вида квадратичного целого, которое является единицей, т. е. общего решения уравнения  $u^2 - Dv^2 = \pm 1$ . Это уравнение почти совпадает с уравнением Пелля  $u^2 - Dv^2 = 1$ , и его решения можно найти почти тем же самым методом, который мы применяли в § 1.9 для нахождения решений уравнения Пелля. Решение задачи нахождения всех единиц (которая представляет собой частный случай  $A_0 = I$  рассматриваемой общей задачи) при  $D > 0$  будет дано в начале следующего параграфа.

Наконец, изменения, которые требуются для рассмотрения случая  $D > 0$ ,  $D \equiv 1 \pmod{4}$ , также незначительны. Если  $A_0$  не делится ни на одно целое, большее 1, то существует такое полуцелое  $r$ , что  $r - \frac{1}{2}\sqrt{D} \equiv 0 \pmod{A_0}$ . Можно считать, что норма  $a_0$  дивизора  $A_0$  по абсолютной величине не превосходит  $\sqrt{D/3}$ . Отсюда следует, что существует по крайней мере одно  $r$ , которое обладает указанным выше свойством и для которого отрицательна

норма  $N(r - \frac{1}{2}\sqrt{D}) = r^2 - \frac{1}{4}D$ . Определим  $r_0$  как наибольшее полуцелое, для которого  $r_0 - \frac{1}{2}\sqrt{D} \equiv 0 \pmod{A_0}$  и  $N(r_0 - \frac{1}{2}\sqrt{D}) < 0$ . Пусть  $A_1$  — такой дивизор, что  $A_0 A_1$  является дивизором  $r_0 - \frac{1}{2}\sqrt{D}$ . При полученном  $A_1$  определим  $A_2$  аналогичным образом. (Существование полуцелого  $r_1$ , для которого  $r_1 - \frac{1}{2}\sqrt{D} \equiv 0 \pmod{A_1}$  и  $N(r_1 - \frac{1}{2}\sqrt{D}) < 0$ , следует из того, что таким полуцелым является  $-r_0$ .) Это даст нам последовательность эквивалентных дивизоров  $A_0 \sim A_1 \sim A_2 \sim \dots$ . В следующем параграфе будет показано, что эта последовательность в конце концов начинает повторяться. Следовательно, можно эффективно определить, найдется ли такое  $i$ , что  $A_i = I$ . Если такое  $i$  найдется, то  $A_0 \sim I$ , и можно использовать цепь эквивалентностей  $A_0 \sim A_1 \sim \dots \sim A_i = I$  для построения квадратичного целого с дивизором  $A_0$ . Тогда дело нахождения *всех* квадратичных целых с дивизором  $A_0$  сводится к делу нахождения *всех единиц*  $u + v\sqrt{D}$ . Последнюю задачу можно решить описанным выше методом, применяя его к  $A_0 = I$ ; это мы тоже докажем в следующем параграфе. Наконец, если последовательность  $A_0 \sim A_1 \sim A_2 \sim \dots$  начинает повторяться, *не достигнув*  $A_i = I$ , то  $A_0$  не является главным дивизором, и это решает нашу задачу, ибо показывает, что нет квадратичных целых с дивизором  $A_0$ .

### Резюме

Пусть  $A$  — заданный дивизор. Мы хотим определить, является ли  $A$  главным дивизором, и, если это так, найти все квадратичные целые с дивизором  $A$ . Не ограничивая общности, можно считать, что  $A$  не делится ни на одно целое, большее 1. Выше мы описали метод построения последовательности дивизоров  $A \sim A_1 \sim A_2 \sim \dots$ , эквивалентных дивизору  $A$ . Этот метод несколько различен в каждом из четырех случаев:  $D < 0$  или  $D > 0$  и  $D \equiv 2$  или  $3 \pmod{4}$  или  $D \equiv 1 \pmod{4}$ . Если  $A_i = I$  для некоторого  $i$ , то  $A$  — главный дивизор. Затем мы решаем задачу определения, является ли  $A$  главным дивизором, следующим образом. Во-первых, доказываем, что *если  $A$  является главным дивизором, то  $A_i = I$  для некоторого  $i$* . Во-вторых, устанавливаем, что за конечное число шагов можно определить, входит ли в полученную последовательность дивизор  $A_i = I$ . При  $D < 0$  выше мы не только доказали эту теорему, но и нашли все единицы, что в этом случае полностью решает нашу задачу. Доказательство теоремы и нахождение всех единиц при  $D > 0$  отложено до следующего параграфа.

## Терминология

Описанный выше метод построения последовательности  $A \sim A_1 \sim A_2 \sim \dots$  мы будем называть *циклическим методом*. Заметим, что в этом методе есть четыре различных случая, и только случай  $D > 0$ ,  $D \not\equiv 1 \pmod{4}$  можно сравнивать с «циклическим методом» из § 1.9. Даже в этом случае наш метод скорее соответствует «английскому методу» из упр. к § 1.9. Действительно, здесь мы выбираем  $r$  так, чтобы  $r^2 - D$  было отрицательным (при как можно большем  $r$ ), а не так, чтобы сделать  $|r^2 - D|$  как можно меньшим ( $r > 0$ ). Однако основная идея совпадает с той, которую использовали древние индийцы; нам кажется уместным напомнить этот факт, употребляя здесь название, которое они дали описанному процессу.

Вычисления при циклическом методе мы будем располагать в виде

$$\begin{array}{ccccccc} r_0 & r_1 & r_2 & \dots & & & \\ a_0 & a_1 & a_2 & a_3 & \dots & & \end{array}$$

Здесь  $a_0$  — норма  $A_0$  и  $r_0 - \sqrt{D}$  делится на  $A_0$ , или, в случае  $D \equiv 1 \pmod{4}$ ,  $r_0$  — полуцелое и  $r_0 - \frac{1}{2}\sqrt{D}$  делится на  $A_0$ . Из теоремы, приведенной в начале параграфа, следует, что  $a_0$  и  $r_0$  однозначно определяют  $A_0$  (упр. 15). Аналогично, для нахождения  $A_j$  достаточно задать  $a_j$  и  $r_j$ . Если  $D \not\equiv 1 \pmod{4}$ , то последовательности  $a_0, a_1, a_2, \dots$  и  $r_0, r_1, r_2, \dots$  образуются по правилам:  $a_{j+1} = (r_j^2 - D)/a_j$  и  $r_{j+1} + r_j \equiv 0 \pmod{a_{j+1}}$ , где  $r_{j+1}$  выбирается среди всех решений сравнения  $r_{j+1} \equiv -r_j \pmod{a_{j+1}}$  по совокупности требований, которые зависят от знака  $D$  и  $r^2 - D$ . (Если  $D < 0$ , то следует сделать  $|r_{j+1}|$  как можно меньшим. В случае  $|r_{j+1}| = \frac{1}{2}a_{j+1}$  надо взять положительное значение  $r_{j+1}$ . При  $D > 0$  попытайтесь сделать отрицательным  $r_{j+1}^2 - D$ . Если это возможно, выберите в качестве  $r_{j+1}$  наибольшее целое, удовлетворяющее условию  $r_{j+1}^2 - D < 0$ . В противном случае сделайте  $|r_{j+1}|$  как можно меньшим). Если  $D \equiv 1 \pmod{4}$ , то надо пользоваться теми же правилами (заменяв  $r^2 - D$  на целое  $r^2 - \frac{1}{4}D$ ).

## Упражнения

Найдите решение задачи данного параграфа (т. е. определите, является ли дивизор  $A$  главным, и, если это так, укажите все квадратичные целые с дивизором  $A$ ) в следующих случаях:

1.  $D = -1$ ,  $A = (5, 2) (13, -5)$ .
2.  $D = -3$ ,  $A = (31, 20)$ .
3.  $D = -2$ ,  $A = (11, 3) (41, 11) (67, 20)$ .

4.  $D = -5$ ,  $A = (23, 8)$ .

5.  $D = -5$ ,  $A = (23, 8)^2$ .

При этом используйте запись

$$\begin{array}{ccccccc} & r_0 & & r_1 & & \dots & \\ a_0 & & a_1 & & a_2 & & \dots, \end{array}$$

предложенную в конце параграфа. Упражнение 3 сделайте двумя способами: во-первых, в качестве отправной точки найдите такое  $r_0$ , что  $A$  делит  $r_0 - \sqrt{-2}$ , и продолжайте вычисления циклическим методом, а во-вторых, решите предложенную задачу для каждого из трех сомножителей  $A$  и перемножьте результаты. Обратите внимание на то, что упр. 5 нельзя решить таким способом.

6. Докажите, что если  $p$  — простое, которое нетривиальным образом делит сумму двух квадратов ( $p$  делит  $x^2 + y^2$ , но не делит ни  $x^2$ , ни  $y^2$ ), то само  $p$  является суммой двух квадратов. [Для этого докажите, что при  $D = -1$  каждый дивизор является главным.]

7. Докажите, что  $p$  делит нетривиальным образом сумму двух квадратов тогда и только тогда, когда  $p = 2$  или  $p \equiv 1 \pmod{4}$ . [«Только тогда» сразу следует из упр. 6. Во второй части используется тот факт, что сравнение  $a^{4n} - 1 \equiv 0 \pmod{p}$  выполняется для всех  $a$  только в том случае, когда  $a^{2n} + 1 \equiv 0 \pmod{p}$  при некотором  $a$ .] Обратите внимание на то, что упр. 6 и 7, по существу, совпадают с теоремами Жирара о суммах двух квадратов (§ 1.7), а их доказательство — с доказательствами Эйлера (2.4).

8. Докажите, что при  $D = -2$  или  $-3$  каждый дивизор является главным, но при  $D = -5$  это утверждение неверно.

В некоторых из следующих упражнений будет удобно использовать сокращения в вычислениях. Предположим, что  $A_0 \sim A_1 \sim \dots \sim A_i = I$ . Пусть  $x_i + y_i \sqrt{D} = 1$ ; возвращаясь назад от этого квадратичного целого, определим  $x_j + y_j \sqrt{D}$  равенством  $(x_j + y_j \sqrt{D})(x_{j+1} - y_{j+1} \sqrt{D}) = r_j - \sqrt{D}$  (или  $r_j - \frac{1}{2}\sqrt{D}$  при  $D \equiv 1 \pmod{4}$ ), или, что то же самое,  $x_j + y_j \sqrt{D} = (r_j - \sqrt{D})(x_{j+1} + y_{j+1} \sqrt{D})/a_{j+1}$ . Тогда  $x_{i-1} + y_{i-1} \sqrt{D} = r_{i-1} - \sqrt{D}$  вообще не требует вычислений и

$$\begin{aligned} x_j + y_j \sqrt{D} &= \frac{[(r_j + r_{j+1}) - (r_{j+1} + \sqrt{D})](x_{j+1} + y_{j+1} \sqrt{D})}{a_{j+1}} = \\ &= n_{j+1}(x_{j+1} + y_{j+1} \sqrt{D}) - (x_{j+2} + y_{j+2} \sqrt{D}) \end{aligned}$$

где  $n_j = (r_{j-1} + r_j)/a_j$ . Если это равенство записать в матричном виде

$$\begin{bmatrix} x_j + y_j \sqrt{D} \\ x_{j+1} + y_{j+1} \sqrt{D} \end{bmatrix} = \begin{bmatrix} n_{j+1} & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_{j+1} + y_{j+1} \sqrt{D} \\ x_{j+2} + y_{j+2} \sqrt{D} \end{bmatrix}$$



то оно приведет к простой формуле

$$\begin{bmatrix} x_0 + y_0 \sqrt{D} \\ x_1 + y_1 \sqrt{D} \end{bmatrix} = \begin{bmatrix} n_1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} n_2 & -1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} n_{i-1} & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_{i-1} - \sqrt{D} \\ 1 \end{bmatrix}$$

для  $x_0 + y_0 \sqrt{D}$ . (При  $D \equiv 1 \pmod{4}$  здесь надо заменить  $r - \sqrt{D}$  на  $r - \frac{1}{2} \sqrt{D}$  с полуцелым  $r$ .)

В следующих упражнениях определите, является ли данный дивизор главным, и, если это так, найдите квадратичное целое с этим дивизором. Считайте известной теорему о том, что если циклический метод не приводит к  $A_i = I$ , то данный дивизор не является главным. (Эту теорему мы докажем в следующем параграфе.)

9.  $D = 67$ ,  $A = (-1, *)$ .

10.  $D = 109$ ,  $A = (-1, *)$ .

11.  $D = 101$ ,  $A = (79, 38)$ .

12.  $D = 79$ ,  $A = (3, 1)^6$ .

13.  $D = -163$ ,  $A = (197, 25)$ .

14.  $D = -165$ ,  $A = (2, *) (5, *) (151, 52)$ .

15. Докажите, что  $a_i$  и  $r_i$  определяют  $A_i$ , т. е. докажите, что если  $A$  и  $A'$  — два дивизора, которые имеют одинаковую норму  $a$  и делят одно и то же квадратичное целое  $r - \sqrt{D}$  (или  $r - \frac{1}{2} \sqrt{D}$  при  $D \equiv 1 \pmod{4}$ ), то  $A = A'$ . Норма  $a$  определяет присутствие или отсутствие множителя  $(-1, *)$ .]

## 7.5. Обоснование циклического метода

Пусть  $A$  — данный дивизор квадратичных целых детерминанта  $D$  ( $D$  свободно от квадратов). При  $D < 0$  задача нахождения всех квадратичных целых с дивизором  $D$  была решена в предыдущем параграфе. При  $D > 0$  мы описали метод решения этой задачи, но применимость этого метода основывалась на недоказанных утверждениях. Данный параграф посвящен доказательству этих утверждений.

Если  $D > 0$  и задан дивизор  $A$  квадратичных целых детерминанта  $D$ , то мы показали, как найти дивизор  $A_0 \sim A$ , который не делится ни на одно целое, большее 1, и имеет норму  $a_0 \leq 2\sqrt{D/3}$  (или  $a_0 \leq \sqrt{D/3}$  при  $D \equiv 1 \pmod{4}$ ). Следовательно, не ограничивая общности, можно предположить, что мы решаем задачу нахождения всех квадратичных целых с дивизором  $A_0$ . (Как частный случай эта задача включает нахождение всех квадратичных целых с дивизором  $I$ , т. е. нахождение всех единиц.)

Сначала предположим, что  $D \equiv 2$  или  $3 \pmod{4}$ . Тогда существует такое целое  $r$ , что  $r \equiv \sqrt{D} \pmod{A_0}$  и  $N(r - \sqrt{D}) < 0$ . Пусть  $r_0$  — наибольшее среди таких целых. Дивизор  $A_1$  опреде-

лим условием:  $A_0 \bar{A}_1$  есть дивизор элемента  $r_0 - \sqrt{D}$ . Тогда найдется такое целое  $r$ , что  $A_1$  делит  $r - \sqrt{D}$  и  $N(r - \sqrt{D}) < 0$ , а именно  $r = -r_0$ . Пусть  $r_1$  — наибольшее среди таких целых; определим дивизор  $A_2$  условием:  $A_1 \bar{A}_2$  есть дивизор элемента  $r_1 - \sqrt{D}$ . Этот процесс можно продолжить и определить последовательность  $A_0 \sim A_1 \sim A_2 \sim \dots$ . Если  $a_j = N(A_j)$ , то последовательности целых чисел  $a_1, a_2, a_3, \dots$  и  $r_1, r_2, r_3, \dots$  можно построить по  $a_0, r_0$ , используя правила:  $a_{i+1} = (r_i^2 - D)/a_i$  и  $r_{i+1}$  — наибольшее целое, удовлетворяющее условиям  $r_{i+1} + r_i \equiv \equiv 0 \pmod{a_{i+1}}$  и  $r_{i+1}^2 - D < 0$ . (Так как  $\bar{A}_{i+1}$  делит  $r_i - \sqrt{D}$ , то  $\sqrt{D} \equiv -r_i \pmod{A_{i+1}}$ . Таким образом, сравнение  $\sqrt{D} \equiv \equiv r_{i+1} \pmod{A_{i+1}}$  эквивалентно сравнению  $r_i + r_{i+1} \equiv \equiv 0 \pmod{A_{i+1}}$ . Поскольку  $A_{i+1}$  не делится ни на одно целое, последнее сравнение, согласно теореме из предыдущего параграфа, эквивалентно сравнению  $r_i + r_{i+1} \equiv 0 \pmod{a_{i+1}}$ .)

**Теорема.** Если  $A_0 \sim I$ , то существует такое  $i > 0$ , что  $N(A_i) = a_i = 1$ . (Другими словами, если  $A_0$  — главный дивизор, то определенная выше последовательность дивизоров  $A_0 \sim A_1 \sim \sim A_2 \sim \dots$  достигает  $A_i = I$ , и техника предыдущего параграфа дает метод нахождения квадратичного целого с дивизором  $A_0$ . Молчаливое предположение, что  $D \equiv 2$  или  $3 \pmod{4}$ , использованное при определении данной последовательности, не является существенным, и, как будет показано ниже, та же самая теорема остается справедливой, если при  $D \equiv 1 \pmod{4}$  сделать естественные изменения в описанном процессе.)

**Доказательство.** Последовательность дивизоров  $A_0 \sim A_1 \sim \sim A_2 \sim \dots$  в конце концов начнет повторяться. Действительно, каждый дивизор  $A_j$  определяет все следующие за ним дивизоры, а неравенство  $|a_j| \leq |a_j a_{j+1}| = |r_j^2 - D| < D$  показывает, что для  $A_j$  имеется только конечное число возможностей. Следовательно, не ограничивая общности, можно считать, что сам  $A_0$  снова встретится в нашей последовательности (для этого достаточно заменить  $A_j$  на  $A_{N+j}$  для некоторого большого  $N$ ). Сделаем это предположение и обозначим через  $k$  наименьшее положительное целое, такое, что  $A_k = A_0$ . Мы должны доказать, что если при таких обстоятельствах  $A_0 \sim I$ , то  $A_i = I$  для некоторого  $i$ ,  $0 \leq i < k$ .

Утверждение  $A_0 \sim I$  означает, что существует квадратичное целое  $x_0 + y_0 \sqrt{D}$  с дивизором  $A_0$ . Умножив его на  $r_0 + \sqrt{D}$  (имеющее дивизор  $\bar{A}_0 A_1$ ) и разделив результат на  $a_0$  (имеющее дивизор  $A_0 \bar{A}_0$ ), мы получим квадратичное целое  $x_1 + y_1 \sqrt{D} = (x_0 + y_0 \sqrt{D})(r_0 + \sqrt{D})/a_0$  с дивизором  $A_1$ . Таким же образом

можно определить последовательность  $x_0 + y_0 \sqrt{D}, x_1 + y_1 \sqrt{D}, \dots$  квадратичных целых  $x_j + y_j \sqrt{D}$  с дивизорами  $A_j$ . Поскольку  $A_k = A_0$ , квадратичные целые  $x_0 + y_0 \sqrt{D}$  и  $x_k + y_k \sqrt{D}$  имеют один и тот же дивизор. Поэтому их частное равно единице, скажем  $x_k + y_k \sqrt{D} = \varepsilon (x_0 + y_0 \sqrt{D})$ . Тогда  $x_{k+1} + y_{k+1} \sqrt{D} = (x_k + y_k \sqrt{D})(r_0 + \sqrt{D})/a_0 = \varepsilon (x_1 + y_1 \sqrt{D})$  и, вообще,  $x_{k+j} + y_{k+j} \sqrt{D} = \varepsilon (x_j + y_j \sqrt{D})$ . Можно воспользоваться периодичностью последовательности  $A_0, A_1, \dots, A_k = A_0$  и определить  $A_j$  для отрицательных  $j$  ( $A_j = A_{j+nk}$  при большом  $n$ ). После этого можно воспользоваться формулой  $x_{j+nk} + y_{j+nk} \sqrt{D} = \varepsilon^n (x_j + y_j \sqrt{D})$  и определить квадратичное целое  $x_j + y_j \sqrt{D}$  с дивизором  $A_j$  при отрицательных  $j$  ( $\varepsilon$  — единица и, следовательно, обратимый элемент). Для доказательства того, что  $A_j = I$  при некотором  $j$ , достаточно доказать, что  $x_j + y_j \sqrt{D} = \pm 1$  при некотором  $j$ . Это можно сделать следующим образом.

Идея предлагаемого доказательства состоит в том, что при большом  $|j|$  как  $|x_j|$ , так и  $|y_j|$  велики, но на одном конце последовательности  $x_j, y_j$  имеют одинаковые знаки, а на другом конце — противоположные. Следовательно, знак  $x_j y_j$  должен где-то измениться. Мы покажем, что из перемены знака  $x_j y_j$  следует существование такого  $j$ , что  $x_j + y_j \sqrt{D} = \pm 1$ .

Основная трудность при этом состоит в доказательстве того, что знак  $x_j y_j$  не может быть одним и тем же для всех  $j$ ; при этом самое трудное — доказать *нетривиальность единицы*  $\varepsilon$ , т. е. что  $\varepsilon \neq \pm 1$ . Мы сделаем это следующим образом.

Согласно определению,

$$\varepsilon = \frac{(r_0 + \sqrt{D})(r_1 + \sqrt{D}) \dots (r_{k-1} + \sqrt{D})}{a_0 a_1 \dots a_{k-1}}. \quad (1)$$

Поэтому, если удастся доказать, что *все целые  $r_j$  положительны* то мы получим, что в представлении  $\varepsilon = u + v \sqrt{D}$  числа  $u$  и  $v$  являются ненулевыми целыми одного знака. Если  $a_j > 0$  для некоторого  $j$ , то  $a_{j+1} < 0$ , так как  $a_j a_{j+1} = r_j^2 - D < 0$ . Кроме того, если  $a_j > 0$ , то  $(r_j + a_j)^2 > D$ , поскольку в противном случае  $r_j$  можно было бы сделать бóльшим. Таким образом,  $r_j^2 - D + 2r_j a_j + a_j^2 > 0$ ,  $a_j (a_{j+1} + 2r_j + a_j) > 0$ ,  $a_{j+1} + 2r_j + a_j > 0$ . Следовательно,  $a_{j+1} (a_{j+1} + 2r_j + a_j) < 0$ ,  $a_{j+1}^2 + 2a_{j+1} r_j + r_j^2 - D < 0$ ,  $(-r_j - a_{j+1})^2 < D$ . Поскольку  $r_{j+1}$  — наибольшее целое, для которого  $r_{j+1} \equiv -r_j \pmod{a_{j+1}}$  и  $r_{j+1}^2 < D$ , мы получаем отсюда, что  $r_{j+1} \geq -r_j - a_{j+1}$ . Тогда  $-r_j \leq r_{j+1} + a_{j+1} \leq r_{j+1}$ . Так как  $r^2 - D < 0$  для  $r = -r_j$  и для  $r = r_{j+1}$ , то отсюда следует, что  $(r_{j+1} + a_{j+1})^2 < D$ . С другой стороны,  $(r_{j+1} - a_{j+1})^2 > D$ , поскольку в противном случае мы

смогли бы увеличить  $r_{j+1}$ . Таким образом,  $(r_{j+1} + a_{j+1})^2 < (r_{j+1} - a_{j+1})^2$ ,  $2r_{j+1}a_{j+1} < -2r_{j+1}a_{j+1}$ ,  $4r_{j+1}a_{j+1} < 0$ ,  $r_{j+1} > 0$ , что и требовалось показать. Если  $a_j < 0$ , то аналогичным образом мы находим, что  $a_{j+1} > 0$ ,  $(r_j - a_j)^2 > D$ ,  $a_{j+1} - 2r_j + a_j < 0$ ,  $(-r_j + a_{j+1})^2 < D$ ,  $r_{j+1} \geq -r_j + a_{j+1}$ ,  $-r_j \leq r_{j+1} - a_{j+1} \leq r_{j+1}$ ,  $(r_{j+1} - a_{j+1})^2 < D$ ,  $(r_{j+1} + a_{j+1})^2 > D > (r_{j+1} - a_{j+1})^2$ ,  $r_{j+1} > 0$ . Таким образом, во всех случаях  $r_j > 0$ , что и требовалось доказать.

Пусть  $\varepsilon = u + v\sqrt{D}$ . Тогда  $u$  и  $v$  — ненулевые целые одного знака и для всех целых  $n$  имеем  $x_{nk} + y_{nk}\sqrt{D} = (x_0 + y_0\sqrt{D})\varepsilon^n$ . Пусть  $\varepsilon^n = U_n + V_n\sqrt{D}$ . Тогда  $U_{n+1} = U_nu + V_nvD$ ,  $V_{n+1} = U_nv + V_nu$ , и по индукции мы получаем отсюда, что  $U_n$  и  $V_n$  — ненулевые целые одного знака при  $n > 0$  и  $|V_{n+1}| > |V_n|$ , так что  $|V_{n+1}|$  сколь угодно велик при большом  $n$ . Далее,

$$x_{nk} = U_nx_0 + DV_ny_0,$$

$$y_{nk} = V_nx_0 + U_ny_0.$$

Если  $x_0$  и  $y_0$  имеют противоположные знаки, то знак  $x_{nk}$  совпадает со знаком наибольшего по абсолютной величине из двух слагаемых  $U_nx_0$  и  $DV_ny_0$ . Мы можем сравнить эти две абсолютные величины, вычитая из квадрата одного слагаемого квадрат другого:

$$\begin{aligned} U_n^2x_0^2 - D^2V_n^2y_0^2 &= (\pm 1 + DV_n^2)x_0^2 - D^2V_n^2y_0^2 = \\ &= \pm x_0^2 + DV_n^2(x_0^2 - Dy_0^2) \end{aligned}$$

(поскольку  $U_n^2 - DV_n^2 = N(\varepsilon^n) = \pm 1$ ). Так как  $x_0^2$  фиксировано, а  $V_n$  сколь угодно велико, то при большом  $n$  последнее выражение имеет тот же знак, что и  $x_0^2 - Dy_0^2$ . Таким образом, знак  $x_{nk}$  совпадает со знаком  $U_nx_0$ , если  $x_0^2 - Dy_0^2 > 0$ , и со знаком  $DV_ny_0$ , если  $x_0^2 - Dy_0^2 < 0$ . Пользуясь тем же методом для нахождения знака  $y_{nk}$ , мы получим, что знак  $y_{nk}$  совпадает со знаком  $V_nx_0$ , если  $0 < V_n^2x_0^2 - U_n^2y_0^2 = V_n^2x_0^2 - (\pm 1 + DV_n^2)y_0^2 = \pm y_0^2 + V_n^2(x_0^2 - Dy_0^2)$  (что справедливо при большом  $n$ , если  $x_0^2 - Dy_0^2 > 0$ ), и совпадает со знаком  $U_ny_0$  при большом  $n$ , если  $x_0^2 - Dy_0^2 < 0$ . Таким образом,  $x_{nk}$  и  $y_{nk}$  имеют один и тот же знак (совпадающий со знаком  $U_nx_0$  и  $V_nx_0$ ), если  $n$  велико и  $x_0^2 - Dy_0^2 > 0$ , и снова имеют один и тот же знак (совпадающий со знаком  $DV_ny_0$  и  $U_ny_0$ ), если  $n$  велико и  $x_0^2 - Dy_0^2 < 0$ . Следовательно, если  $x_0$  и  $y_0$  имеют противоположные знаки, то  $x_{nk}$  и  $y_{nk}$  имеют одинаковые знаки при всех достаточно больших  $n$ . Если  $x_0$  и  $y_0$  имеют одинаковые знаки, то  $x_{-nk} + y_{-nk}\sqrt{D} = (x_0 + y_0\sqrt{D})\varepsilon^{-n}$ ,  $x_{-nk} - y_{-nk}\sqrt{D} = \pm (x_0 - y_0\sqrt{D})\varepsilon^n$  и, поскольку знаки  $x_0$  и  $-y_0$  противоположны, приведенное выше доказательство показывает, что  $x_{-nk}$  и  $-y_{-nk}$  при всех достаточно больших  $n$  имеют одинаковые знаки. Таким образом, и в этом случае знак  $x_jy_j$  при-

нимает оба значения. Следовательно, либо  $x_j y_j = 0$  для некоторого  $j$ , либо найдется такое  $j$ , что  $x_j y_j$  и  $x_{j+1} y_{j+1}$  имеют противоположные знаки.

Вторая из этих двух альтернатив невозможна, поскольку  $x_{j+1} + y_{j+1} \sqrt{D} = (x_j + y_j \sqrt{D})(r_j + \sqrt{D})/a_j$ ,  $(x_{j+1} + y_{j+1} \sqrt{D}) \times (x_j - y_j \sqrt{D}) = r_j + \sqrt{D}$ , откуда следует, что  $x_j y_{j+1} - x_{j+1} y_j = 1$ . Если два целых числа имеют противоположные знаки, то их разность не меньше 2; следовательно, из последнего равенства мы получаем, что  $x_j y_{j+1} x_{j+1} y_j \geq 0$ , поэтому  $x_j y_j$  и  $x_{j+1} y_{j+1}$  не могут иметь противоположные знаки. Таким образом,  $x_j y_j = 0$  по меньшей мере для одного значения  $j$ . Тогда, с одной стороны, разность  $x_{j+1} x_j - D y_j y_{j+1}$  равна  $r_j$  (согласно формуле  $(x_{j+1} + y_{j+1} \sqrt{D})(x_j - y_j \sqrt{D}) = r_j + \sqrt{D}$ ), а с другой стороны, она равна или  $x_{j+1} x_j$ , или  $-D y_j y_{j+1}$  (поскольку  $x_j$  или  $y_j$  равно нулю). Так как  $|r_j| < \sqrt{D} < D$ , то второе из этих равенств невозможно. Следовательно,  $y_j = 0$  и  $1 = x_j y_{j+1} - x_{j+1} y_j = x_j y_{j+1}$ , поэтому  $x_j$  и  $y_{j+1}$  равны  $\pm 1$ . Таким образом,  $x_j + y_j \sqrt{D} = \pm 1$  и  $A_j = I$ , что и требовалось доказать. Это завершает доказательство теоремы.

**Теорема.** Если  $D \equiv 2$  или  $3 \pmod{4}$  и  $A_0 = I$ , то, согласно предыдущей теореме, применение циклического метода к  $A_0$  приведет нас снова к  $I$ . Пусть  $k$  — наименьшее положительное целое, такое, что  $a_k = \pm 1$ , и пусть  $\varepsilon$  определено равенством (1). Тогда единицы среди квадратичных целых детерминанта  $D$  в точности совпадают с квадратичными целыми  $\pm \varepsilon^n$  при целом  $n$ .

**Доказательство.** Применить циклический метод к  $A$  — то же самое, что применить его к  $(-1, *) A$  и умножить полученный результат на  $(-1, *)$ . Следовательно, дивизор  $(-1, *)$  является главным тогда и только тогда, когда применение циклического метода к  $A_0 = I$  приводит к  $(-1, *)$ , прежде чем снова к  $I$ . Таким образом, определенное в теореме  $\varepsilon$  имеет дивизор  $(-1, *)$ , если  $(-1, *)$  является главным дивизором; в противном случае дивизор  $\varepsilon$  равен  $I$ . В частности, это  $\varepsilon$  всегда является единицей. Если  $x_0 + y_0 \sqrt{D}$  — произвольная единица, то построенная при помощи циклического метода последовательность  $x_j + y_j \sqrt{D}$  содержит  $\pm 1$ . Дивизор элемента  $x_0 + y_0 \sqrt{D}$  равен  $I$  или  $(-1, *)$ . Тогда дивизор каждого  $x_j + y_j \sqrt{D}$  равен либо  $A_j$ , либо  $(-1, *) A_j$ , где  $\dots, A_{-1}, I_1, A_1, A_2, \dots$  — цикл дивизоров, полученный применением циклического метода к  $I$ . Кроме того,  $x_{j+k} + y_{j+k} \sqrt{D} = \varepsilon (x_j + y_j \sqrt{D})$ , и норма  $x_j + y_j \sqrt{D}$  равна  $\pm a_j$ . Поскольку  $a_j = \pm 1$  в том и только в том случае, когда  $j$  кратен  $k$ , из равенства  $x_j + y_j \sqrt{D} = \pm 1$  следует, что  $\varepsilon^n (x_0 + y_0 \sqrt{D}) = \pm 1$  и  $x_0 + y_0 \sqrt{D} = \pm \varepsilon^{-n}$ , что и требовалось показать.



Все единицы  $\pm \varepsilon^n$  различны, так как из равенства  $\pm \varepsilon^n = \pm \varepsilon^m$  при  $m \neq n$  следовало бы, что  $\varepsilon^\mu = \pm 1$  при некотором положительном  $\mu$ , в противоречие тому, что  $\varepsilon^\mu = U_\mu + V_\mu \sqrt{D}$ , где  $U_\mu$  и  $V_\mu$  — ненулевые целые одинакового знака. Следовательно, последняя теорема дает простую формулу для единицы самого общего вида и позволяет найти в общем виде квадратичное целое с дивизором  $A$ , если известно хотя бы одно квадратичное целое, имеющее дивизор  $A$ . Первая из этих теорем показывает, что если  $A_0$  — дивизор квадратичного целого, то  $A_j = I$  для некоторого  $j$  с  $0 \leq j < k$ , и, поскольку квадратичное целое с дивизором  $I$  известно, цепочка эквивалентностей  $A_0 \sim A_1 \sim \dots \sim A_j = I$  дает возможность легко найти квадратичное целое с дивизором  $A_0$ .

В случае  $D > 0$ ,  $D \equiv 2$  или  $3 \pmod{4}$  это полностью решает задачу определения, является ли данный дивизор главным, и, если это верно, задачу нахождения всех квадратичных целых с этим дивизором. Нам осталось рассмотреть лишь случай  $D > 0$ ,  $D \equiv 1 \pmod{4}$ . По существу, он совпадает с только что разобранным случаем, поэтому ограничимся лишь краткими указаниями. Как было показано в предыдущем параграфе, каждый дивизор  $A$  эквивалентен некоторому  $A_0$  с нормой, не превосходящей  $\sqrt{D/3}$ .

Тогда найдется такое полуцелое  $r$ , что  $r - \frac{1}{2} \sqrt{D} \equiv 0 \pmod{A_0}$

и  $N \left( r - \frac{1}{2} \sqrt{D} \right) < 0$ . Пусть  $r_0$  — наибольшее такое полуцелое,

и пусть дивизор  $A_1$  определен условием:  $A_0 \bar{A}_1$  — дивизор элемента  $r_0 - \frac{1}{2} \sqrt{D}$ . Тогда существуют такие полуцелые  $r$  (например,

$r = -r_0$ ), что  $r - \frac{1}{2} \sqrt{D} \equiv 0 \pmod{A_1}$  и  $N \left( r - \frac{1}{2} \sqrt{D} \right) < 0$ .

Пусть  $r_1$  — наибольшее такое  $r$ ; продолжим процесс таким образом, чтобы получить последовательность  $A_0 \sim A_1 \sim A_2 \sim \dots$ .

Мы должны показать, что если  $A_0 \sim I$ , то  $A_i = I$  для некоторого  $i > 0$ . Доказательство в точности совпадает с тем, которое было приведено в предыдущем случае, за исключением доказательства того, что  $x_j y_j$  и  $x_{j+1} y_{j+1}$  не могут иметь противоположные знаки. Из равенства  $(x_{j+1} + y_{j+1} \sqrt{D})(x_j - y_j \sqrt{D}) =$

$= r_j + \frac{1}{2} \sqrt{D}$  следует, что  $x_j y_{j+1} - x_{j+1} y_j = \frac{1}{2}$ ,  $(2x_j)(2y_{j+1}) -$

$-(2x_{j+1})(2y_j) = 2$ . Поскольку  $2x_j, 2y_j, 2x_{j+1}, 2y_{j+1}$  — целые,

мы получаем отсюда, что  $x_j y_{j+1}$  и  $x_{j+1} y_j$  всегда имеют одинаковые знаки, за исключением того случая, когда одно из них равно нулю или  $|(2x_j)(2y_{j+1})| = |(2x_{j+1})(2y_j)| = 1$ . В последнем слу-

чае все  $x_j, y_j, x_{j+1}, y_{j+1}$  равны  $\pm 1/2$ . Но тогда  $N \left( r_j + \frac{1}{2} \sqrt{D} \right) =$

$= N(x_j + y_j \sqrt{D}) N(x_{j+1} + y_{j+1} \sqrt{D}) = \left[ \left( \frac{1}{2} \right)^2 - D \left( \frac{1}{2} \right)^2 \right]^2 > 0$ ,

что противоречит предположению.



Основная единица  $\varepsilon$  в случае  $D \equiv 1 \pmod{4}$  находится при помощи очевидной модификации приведенной выше теоремы для случая  $D \equiv 2$  или  $3 \pmod{4}$ , а именно:

**Теорема.** Пусть  $D \equiv 1 \pmod{4}$  ( $D$  свободно от квадратов и положительно). Если  $A_0 = I$  и если

$$\varepsilon = \frac{(r_0 + \frac{1}{2} \sqrt{D})(r_1 + \frac{1}{2} \sqrt{D}) \dots (r_{k-1} + \frac{1}{2} \sqrt{D})}{a_0 a_1 \dots a_{k-1}},$$

где  $a_j$  и  $r_j$  получены циклическим методом и где  $k$  — наименьшее положительное целое, для которого  $a_k = \pm 1$ , то единицами являются квадратичные целые  $\pm \varepsilon^n$  с целым  $n$ .

### Упражнения

1. Найдите все единицы среди квадратичных целых детерминанта  $D = 61$ . Сравните с решением уравнения Пелля  $x^2 = 61y^2 + 1$ .

2. Найдите все единицы среди квадратичных целых детерминанта  $D = 109$ .

## 7.6. Группа классов дивизоров: примеры

В гл. 5 были определены понятия «числа классов» и «системы представителей», но при этом мы не пытались ни вычислить число классов (что трудно даже для  $\lambda = 11$ ), ни найти систему представителей. Так как циклический метод дает такой простой способ определения, является ли главным данный дивизор, то в случае дивизоров квадратичных целых решение обеих задач совершенно элементарно.

В качестве первого примера рассмотрим случай  $D = 67$ . Поскольку  $D \equiv 3 \pmod{4}$ , каждый дивизор эквивалентен дивизору с нормой, не превосходящей  $2\sqrt{67/3} < 10$ , который не делится ни на одно целое, большее 1. Среди простых 2, 3, 5, 7, заключенных в этих границах, 2 разветвляется ( $67 \equiv 3 \pmod{4}$ ), 3 распадается ( $67 \equiv 1 = 1^2 \pmod{3}$ ), 5 остается простым ( $67 \equiv 2 \not\equiv n^2 \pmod{5}$ , поскольку  $n^2 \equiv 0, 1, 4 \pmod{5}$ ) и 7 распадается ( $67 \equiv 4 = 2^2 \pmod{7}$ ). Кроме того, поскольку  $D > 0$ , рассуждения из § 7.3 требуют рассмотрения дивизора  $(-1, *)$  с нормой  $-1$ . Таким образом, каждый дивизор эквивалентен одному из дивизоров  $I, (2, *), (3, \pm 1), (2, *), (3, \pm 1), (7, \pm 2), (3, \pm 1)^2$  или  $(-1, *)$ , умноженному на один из перечисленных выше. Применяя циклический метод к  $(-1, *)$ , мы получим

$$\begin{array}{cccccccccccc} r = & 8 & 7 & 5 & 2 & 7 & 7 & 2 & 5 & 7 & 8 & 8 \\ a = & -1 & 3 & -6 & 7 & -9 & 2 & -9 & 7 & -6 & 3 & -1 \end{array}$$

после чего  $r$  и  $a$  начинают повторяться. Поскольку мы не достигли  $a = 1$ , дивизор  $(-1, *)$  не является главным, и число классов не меньше двух. С другой стороны, приведенные выше вычисления дают эквивалентности  $(-1, *) \sim (3, 1) \sim (-1, *) (2, *) (3, 2) \sim (7, 2) \sim (-1, *) (3, 1)^2 \sim (2, *) \sim (-1, *) (3, 2)^2 \sim (7, -2) \sim (-1, *) (2, *) (3, 1) \sim (3, -1)$ . (Например,  $a_4 = -9$ , поэтому  $A_4$  — дивизор с нормой  $-9$ . Он не делится на 3. Следовательно, этот дивизор имеет вид  $(-1, *) (3, \pm 1)^2$ . Поскольку он делит  $r_4 - \sqrt{67} = 7 - \sqrt{67}$ , он должен быть равен  $(-1, *) \times (3, 1)^2$ ). Умножая эти эквивалентности на  $(-1, *)$ , получим  $I \sim (-1, *) (3, 1) \sim (2, *) (3, 2) \sim \dots \sim (-1, *) (3, -1)$ . При этом мы получаем все приведенные выше дивизоры, поэтому число классов равно 2 и дивизоры  $I, (-1, *)$  образуют систему представителей. Кроме того, как показывают эти эквивалентности,  $I \sim (7, \pm 2)^2, (-1, *) \sim (2, *) \sim (3, \pm 1) \sim (7, \pm 2)$ ; поскольку отношение эквивалентности дивизоров согласовано с умножением, мы вновь получаем отсюда все приведенные выше эквивалентности, например:

$$(-1, *) (2, *) (3, 2) \sim (-1, *) (-1, *) (-1, *) \sim (-1, *).$$

В качестве второго примера рассмотрим случай  $D = -165$ . Здесь 2 разветвляется ( $D \equiv 3 \pmod{4}$ ), 3 разветвляется, 5 разветвляется, 7 остается простым ( $-165 \equiv 3 \pmod{7}$ , и по модулю 7 квадраты сравнимы с 0, 1, 2, 4), 11 разветвляется и 13 распадается ( $-165 \equiv 4 = 2^2 \pmod{13}$ ). С другой стороны, каждый дивизор эквивалентен дивизору с нормой, меньшей  $2\sqrt{165/3} = \sqrt{220} < 15$ . Таким образом, каждый дивизор эквивалентен по крайней мере одному из дивизоров  $I, (2, *), (3, *), (5, *), (2, *) (3, *), (2, *) (5, *), (11, *), (13, \pm 2)$ . Применяя процесс приведения к любому из этих дивизоров, мы получим дивизор с большей нормой, например:  $(2, *) (5, *)$  делит  $5 - \sqrt{-165}$ , имеющее норму 190, поэтому  $(2, *) (5, *) \sim (19, -5)$ . Исключение составляют дивизоры  $(13, \pm 2)$ . Так как  $(13, 2)$  делит  $2 - \sqrt{-165}$ , но 13 не делит  $2 - \sqrt{-165}$ , и так как  $N(2 - \sqrt{-165}) = 13^2$ , то дивизор элемента  $2 - \sqrt{-165}$  равен  $(13, 2)^2$  и  $(13, 2) \sim (13, -2)$ . Следовательно, приведенный выше список из 9 дивизоров дает нам, если исключить из него один из двух дивизоров  $(13, \pm 2)$ , список из 8 дивизоров, среди которых только  $I$  является главным, и каждый дивизор эквивалентен по крайней мере одному из этих 8 дивизоров.

В этом случае легко найти групповую, т. е. мультипликативную, структуру на множестве классов дивизоров. Пусть  $A = (2, *)$ ,  $B = (3, *)$  и  $C = (5, *)$ . Тогда  $A^2 \sim B^2 \sim C^2 \sim I$ ,  $AB = (2, *) (3, *)$  и  $AC = (2, *) (5, *)$ . Класс  $BC$  можно найти, заме-

тив, что дивизор  $\sqrt{-165}$  равен  $(3, *) (5, *) (11, *)$ , так что  $BC \sim \sim (11, *) B^2 C^2 \sim (11, *)$ . Тогда  $ABC$  должен быть эквивалентен оставшемуся дивизору:  $ABC \sim (13, \pm 2)$ , поскольку в противном случае он был бы эквивалентен другому из этих дивизоров и отсюда следовало бы, что один из них является главным. (Например, если  $ABC \sim B$ , то  $AC \sim AB^2 C \sim B^2 \sim I$  — в противоречие тому, что  $(2, *) (5, *)$  не является главным дивизором.) Аналогично, никакие 2 из 8 дивизоров  $I, A, B, C, AB, BC, AC$  и  $ABC$  не могут быть эквивалентными. Таким образом, число классов равно 8 и приведенные выше 8 дивизоров образуют систему представителей. (Конечно, легко и непосредственно доказать, что  $ABC \sim \sim (13, \pm 2)$ ; см. упр. 7.)

Случай  $D = -163$  приводит к совершенно другому результату. Поскольку  $D \equiv 1 \pmod{4}$ , каждый дивизор эквивалентен дивизору с нормой, не превосходящей  $\sqrt{163/3} < 8$ . В этом случае 2 остается простым ( $D \equiv 5 \pmod{8}$ ), 3 остается простым ( $D \equiv \equiv -1 \pmod{3}$ ), 5 остается простым ( $D \equiv 2 \pmod{5}$ ) и 7 остается простым ( $D \equiv 5 \pmod{7}$ ). Следовательно, единственными дивизорами с нормой  $< 8$  являются главные дивизоры  $I$  и  $(2)$ , число классов равно 1, а систему представителей образует  $I$ . Таким образом, для квадратичных целых детерминанта  $D = -163$  имеет место однозначность разложения на множители. Отсюда следует знаменитая теорема Эйлера о том, что при  $x = 0, 1, 2, \dots, 39$  число  $x^2 + x + 41$  является простым (см. упр. 8).

Случай  $D = 79$  Гаусс часто использовал в качестве примера <sup>1)</sup> (Disquisitiones Arithmeticae, Arts. 185, 186, 187, 195, 196, 198, 205, 223). При  $D = 79$  каждый дивизор эквивалентен дивизору с нормой, не превосходящей  $2\sqrt{79/3} < 11$ . Такой дивизор должен быть произведением дивизоров  $(-1, *)$ ,  $(2, *)$ ,  $(3, \pm 1)$ ,  $(5, \pm 2)$ ,  $(7, \pm 3)$ . Вычисление, которое нужно произвести для того, чтобы выяснить, является ли дивизор  $(-1, *)$  главным, показывает, что

$$\begin{array}{cccccc} r = & 8 & 7 & 7 & 8 \\ a = & -1 & 15 & -2 & 15 & -1 \end{array}$$

Следовательно,  $(-1, *)$  не является главным дивизором. В то же время из этого вычисления следует, что  $(-1, *) \sim (-1, *) (2, *)$ , поэтому  $I = (-1, *)^2 \sim (2, *)$ , т. е.  $(2, *)$  — главный дивизор. Действительно,  $(2, *)$  — дивизор элемента  $9 - \sqrt{79}$ . Произве-

<sup>1)</sup> Случай  $D = 79$  интересен потому, что 79 является наименьшим положительным детерминантом, для которого род содержит более одного класса дивизоров. (Определение рода см. в § 7.9.) Этим обстоятельством объясняется контрпример Лагранжа, опровергающий гипотезу Эйлера о простых вида  $x^2 - Dy^2$  при  $D = 79$  (см. упр. 8 к § 7.9). Интерес Гаусса к случаю  $D = 79$ , по-видимому, связан с контрпримером Лагранжа.

дем вычисления для того, чтобы выяснить, является ли главным дивизор  $(3, 1)$ :

$$\begin{array}{cccccccc} r = & 7 & 3 & 4 & 5 & 7 & 8 & 7 \\ a = & 3 & -10 & 7 & -9 & 6 & -5 & 3 \end{array}$$

Следовательно,  $(3, 1)$  — не главный дивизор и  $(3, 1) \sim (-1, *) \times \times (2, *) (5, -2) \sim (7, -3) \sim (-1, *) (3, -1)^2 \sim (2, *) (3, 1) \sim \sim (-1, *) (5, -2)$ . Пусть  $A = (-1, *)$  и  $B = (3, 1)$ . Тогда  $B \sim \sim A\bar{B}^2$ ,  $B^3 \sim A (B\bar{B})^2 \sim A$ . Таким образом,  $B^6 \sim I$ , но  $B^3 \not\sim I$ . Далее, если  $B^2 \sim I$ , то  $B \sim A\bar{B}^2 \sim A$ ,  $AB \sim I$ . Но вычисление, которое надо произвести для того, чтобы выяснить, является ли главным дивизор  $AB = (-1, *) (3, 1)$ , совпадает с проведенным выше вычислением, если изменить в нем знаки при  $a$  на противоположные. Следовательно,  $AB \not\sim I$ ,  $A \not\sim B$ ,  $B^2 \not\sim I$ . Таким образом,  $I, B, B^2, B^3, B^4, B^5$  — шесть неэквивалентных <sup>1)</sup> дивизоров. Кроме того,  $(-1, *) \sim B^3$ ,  $(2, *) \sim I$ ,  $(3, 1) = B$ ,  $(3, -1) = \bar{B} \sim B^5$ ,  $(5, -2) \sim B^4$  (поскольку из эквивалентности  $(3, 1) \sim (-1, *) (5, -2)$  следует, что  $(5, -2) \sim (-1, *) \times \times (3, 1) \sim B^4$ ),  $(5, 2) \sim B^2$ ,  $(7, -3) \sim B$  (так как  $A_2 = (7, -3)$  во втором из вычислений, проведенных выше),  $(7, 3) \sim B^5$ . Следовательно, число классов равно 6, а  $I, B, B^2, B^3, B^4, B^5$  является системой представителей; здесь  $B = (3, 1)$ .

Системы представителей следует выбирать таким образом, чтобы легко было описать таблицу умножения. Например, в предыдущем случае таблицу умножения полностью описывает формула  $B^6 \sim I$ ; ту же роль играют соотношения  $A^2 \sim I$ ,  $B^2 \sim I$ ,  $C^2 \sim I$  при  $D = -165$ . Несколько менее очевидно, как сделать это при  $D = -161$  <sup>2)</sup>. В этом случае 2 разветвляется ( $-161 \equiv 3 \pmod{4}$ ), 3 распадается ( $-161 \equiv 1 \pmod{3}$ ), 5 распадается ( $-161 \equiv 4 \pmod{5}$ ), 7 разветвляется ( $-161 \equiv 0 \pmod{7}$ ), 11 распадается ( $-161 \equiv 4 \pmod{11}$ ) и 13 остается простым ( $-161 \equiv 8 \equiv -5 \pmod{13}$ ), а квадраты по модулю 13 равны 1, 4, 9  $\equiv -4, 3, -1, -3$ ). Таким образом, дивизорами с нормой, меньшей  $2\sqrt{|D|/3} < 15$ , не делящимися ни на одно целое, большее 1, являются  $I, (2, *), (3, 1), (3, -1), (5, 2), (5, -2), (2, *) (3, 1), (2, *) (3, -1), (7, *), (3, 1)^2, (3, -1)^2, (2, *) (5, 2), (2, *) \times \times (5, -2), (11, 2), (11, -2), (2, *) (7, *)$ . Каждый дивизор эквивалентен по крайней мере одному из этих 16 дивизоров.

<sup>1)</sup> Из  $B^4 \sim I$  следовало бы, что  $B^2 \sim B^2 B^6 \sim (B^4)^2 \sim I$ , поэтому  $B^4 \not\sim I$ . Аналогично, если  $B^5 \sim I$ , то  $B \sim B \cdot B^5 \sim I$ , что невозможно. Поэтому никакие два из дивизоров  $B^0, B^1, \dots, B^5$  не эквивалентны, ибо в противном случае при некотором  $j$ ,  $0 < j < 6$ , дивизор  $B^j$  был бы эквивалентен  $I$ .

<sup>2)</sup> Этот случай рассмотрел Гаусс в разд. 307 «Арифметических исследований».

Легко проверить, что ни один из этих 16 дивизоров, кроме  $I$ , не является главным. (Например,  $(11, 2)$  делит квадратичное целое  $2 - \sqrt{-161}$ , имеющее норму  $165 = 11 \cdot 15$ , и циклический метод не приводит  $(11, 2)$  к главному дивизору.) Пусть  $A = (3, 1)$ . Тогда  $A^2$  содержится среди этих 16 дивизоров, но  $A^3$  не принадлежит к их числу. Приведение  $A^3$  дает

$$\begin{aligned} r &= 1 & -1 \\ a &= 27 & 6 \end{aligned}$$

и  $A^3 \sim (2, *) (3, -1)$ . Таким образом,  $A^4 \sim (2, *) (3, -1) \times (3, 1) \sim (2, *)$ ,  $A^5 \sim (2, *) (3, 1)$ ,  $A^6 \sim (2, *)^2 (3, -1)^2 \sim (3, -1)^2$  и  $A^7 \sim (3, -1)^2 (3, 1) \sim (3, -1)$  не являются главными дивизорами, но  $A^8 \sim I$ . Однако не каждый дивизор эквивалентен некоторой степени  $A$ . Точнее,  $(7, *)$  является дивизором, квадрат которого — главный дивизор. Следовательно,  $(7, *)$  не может быть эквивалентен ни одной степени  $A$ , отличной от  $I$  или  $A^4$ , но, поскольку  $A^4 \sim (2, *)$ , а ни  $(7, *)$ , ни  $(7, *) (2, *)$  не являются главными дивизорами,  $(7, *)$  не эквивалентен ни одной степени  $A$ . Пусть  $B = (7, *)$ . Тогда, как и при доказательстве теоремы Ферма, мы получаем, что дивизоры  $B, BA, BA^2, \dots, BA^7$  не эквивалентны друг другу и не эквивалентны  $I, A, A^2, \dots, A^7$ . Таким образом, имеются по меньшей мере 16 неэквивалентных дивизоров и 16 приведенных выше дивизоров должны быть не эквивалентны, причем каждый из них должен быть эквивалентен единственному дивизору вида  $A^i B^j$  ( $i = 0, 1, \dots, 7; j = 0, 1$ ). Точнее, дивизор  $AB = (3, 1) (7, *)$  циклическим методом

$$\begin{aligned} r &= 7 & 3 \\ a &= 21 & 10 & 17 \end{aligned}$$

приводится к виду  $AB \sim (2, *) (5, -2)$ . Аналогично,  $A^2 B \sim (3, 1) (2, *) (5, -2) \sim (11, -2)$ ,  $A^3 B \sim (3, 1) (11, -2) \sim (5, 2)$ ,  $A^4 B \sim (2, *) (7, *)$ ,  $A^5 B \sim A^3 \overline{B} \sim (5, -2)$ ,  $A^6 B \sim (11, 2)$ ,  $A^7 B \sim (2, *) (5, 2)$ .

Короче говоря, при  $D = -161$  16 дивизоров  $A^i B^j$  ( $i = 0, 1, \dots, 7; j = 0, 1$ ) образуют систему представителей; здесь  $A = (3, 1)$ ,  $B = (7, *)$  и  $A^8 \sim I$ ,  $B^2 \sim I$ . На языке теории групп можно сказать, что в данном случае группа классов дивизоров является абелевой группой, порожденной двумя (независимыми) образующими  $A$  и  $B$  порядков 8 и 2 соответственно. Преимущество системы представителей  $\{A^i B^j\}$  над приведенной выше системой  $(2, *)$ ,  $(3, \pm 1)$ ,  $\dots$  очевидно. Как только несколько простых дивизоров выражены через  $A$  и  $B$ :  $(2, *) \sim A^4$ ,  $(3, 1) \sim A$ ,  $(5, 2) \sim A^3 B$ ,  $(7, *) \sim B$ ,  $(11, 2) \sim A^6 B$ , — легко вычислить

класс любого дивизора. Например,  $(3, -1) (11, 2)^2 \sim A^{-1} (A^6 B)^2 \sim \sim A^3$ . Несложно провести классификацию и других простых дивизоров. Например,  $(17, 3) \sim (2, *) (5, 2) \sim A^4 A^3 B = A^7 B$ ,  $(23, *) \sim (7, *) \sim B$ ,  $(29, 10) \sim (3, -1)^2 \sim A^{-2} \sim A^6$  и т. д.

В качестве последнего примера рассмотрим случай  $D = 985$ . Здесь  $D \equiv 1 \pmod{4}$ , на самом деле  $D \equiv 1 \pmod{8}$ . Следовательно, 2 распадается. Производя вычисления, для того чтобы установить, является ли  $(2, 0)$  главным дивизором ( $(2, 0)$  — простой дивизор, деляющий 2, по модулю которого  $\omega = \frac{1}{2} - \frac{1}{2} \sqrt{985} \equiv 0$ ), получим

$$\begin{array}{cccccccccccc} r = & \frac{29}{2} & \frac{7}{2} & \frac{19}{2} & \frac{29}{2} & \frac{31}{2} & \frac{29}{2} & \frac{7}{2} & \frac{19}{2} & \frac{29}{2} & \frac{31}{2} & \frac{29}{2} \\ a = 2 & -18 & 13 & -12 & 3 & -2 & 18 & -13 & 12 & -3 & 2 \end{array}$$

Отсюда не только следует, что  $(2, 0)$  не является главным дивизором; мы получаем также, что дивизор  $(-1, *)$  — главный (действительно,  $(2, 0) \sim (-1, *) (2, 0)$ ) и что  $(2, 0) \sim (2, 1) (3, 1)^2 \sim \sim (13, 6) \sim (2, 0)^2 (3, -1) \sim (3, 1)$ . Вычисление с целью определить, является ли главным дивизор  $(5, *)$ , дает таблицу

$$\begin{array}{cccccccccccc} r = & \frac{25}{2} & \frac{11}{2} & \frac{13}{2} & \frac{21}{2} & \frac{27}{2} & \frac{21}{2} & \frac{13}{2} & \frac{11}{2} & \frac{25}{2} & \frac{25}{2} \\ a = 5 & -18 & 12 & -17 & 8 & -8 & 17 & -12 & 18 & -5 \end{array}$$

Отсюда следует, что  $(5, *)$  — не главный дивизор. Кроме того,  $(5, *) \sim (2, 1) (3, -1)^2 \sim (2, 0)^2 (3, 1) \sim (17, 4) \sim (2, 1)^3 \sim \sim (2, 0)^3 \sim (17, -4) \sim \dots$ . Таким образом,  $(2, 0)^6 \sim (5, *)^2 \sim \sim I$ . Пусть  $A = (2, 0) \sim (3, 1)$ . Тогда дивизор  $A^3$  не является главным, но  $A^6$  — главный дивизор. Легко проверить, что  $A^2$  не является главным дивизором:

$$\begin{array}{cccccccc} r = & \frac{25}{2} & \frac{5}{2} & \frac{27}{2} & \frac{29}{2} & \frac{25}{2} & \frac{15}{2} & \frac{23}{2} & \frac{25}{2} \\ a = 6 & -15 & 16 & -4 & 9 & -10 & 19 & -6 \end{array}$$

Отсюда следует, что дивизоры  $I, A, A^2, A^3, A^4, A^5$  не эквивалентны. Кроме того,  $(-1, *) \sim I$ ,  $(2, 0) \sim A$ ,  $(2, 1) \sim A^5$ ,  $(3, 1) \sim \sim A$ ,  $(3, -1) \sim A^5$ ,  $(5, *) \sim A^3$ ,  $(13, 6) \sim A$ ,  $(13, -6) \sim A^5$ ,  $(17, \pm 4) \sim \sim A^3$ . Каждый дивизор эквивалентен дивизору с нормой  $< \sqrt{D/3} < < \sqrt{330} < 19$ . Таким образом, каждый дивизор эквивалентен произведению простых дивизоров, нормы которых меньше 19. Если мы докажем, что не существует простых дивизоров с нормой



7 или 11, т. е. что 7 или 11 остаются простыми, то из приведенного выше будет следовать, что каждый дивизор эквивалентен некоторой степени  $A$ . Сравнения  $985 \equiv 5 \not\equiv x^2 \pmod{7}$ ,  $985 \equiv -5 \equiv -4^2 \pmod{11}$ ,  $-1 \not\equiv x^2 \pmod{11}$  показывают, что 7 и 11 остаются простыми дивизорами. Таким образом, число классов равно 6 и каждый дивизор эквивалентен некоторой степени  $A$ ; здесь  $A = (2, 0)$  и  $A^6 \sim I$ .

### Упражнения

Каждый из следующих случаев разберите по образцу примеров в тексте, т. е. найдите систему представителей и составьте таблицу умножения в как можно более простой форме.

- |                 |                 |
|-----------------|-----------------|
| 1. $D = 61$ .   | 4. $D = 305$ .  |
| 2. $D = -235$ . | 5. $D = -129$ . |
| 3. $D = 145$ .  | 6. $D = -105$ . |

7. Воспользуйтесь циклическим методом для доказательства того, что  $(2, *) (3, *) (5, *) \sim (13, \pm 2)$  при  $D = -165$ .

8. Докажите, что при  $x = 0, 1, \dots, 39$  число  $x^2 + x + 41$  является простым. [Любой простой делитель числа  $x^2 + x + 41$  должен распадаться в квадратичных целых детерминанта  $-163$ . Поскольку каждый дивизор является главным, справедливо равенство  $\frac{1}{2}[(2x + 1) + \sqrt{-163}] = (r + s\sqrt{-163})(u + v\sqrt{-163})$ , где  $r^2 + 163s^2$  — данный простой делитель числа  $x^2 + x + 41$ . Это дает:  $(2r)(2v) + (2s)(2u) = 2$ . Обычно два слагаемых в последней сумме имеют противоположные знаки; это означает, что слагаемые в  $ru - 163sv = \frac{1}{2}(2x + 1)$  имеют один и тот же знак. В этом случае из неравенства  $x \geq 0$  следует неравенство  $x \geq 40\frac{1}{2}$ . Если  $rsuv = 0$ , то  $v = 0$ ,  $u = \pm 1$  и  $x^2 + x + 41 = r^2 + 163s^2$  — простое число, что и требуется.]

### 7.7. Группа классов дивизоров: общая теорема

Техника, которой мы пользовались в предыдущем параграфе для проверки эквивалентности дивизоров  $A$  и  $B$ , заключалась в применении циклического метода к дивизору  $A\bar{B}$ , для того чтобы установить, является ли  $A\bar{B}$  главным дивизором. Однако есть и другой, обычно лучший, метод проверки эквивалентности  $A \sim B$ . Предположим, что мы применяем циклический метод отдельно к дивизорам  $A$  и  $B$  и получаем две последовательности  $A \sim A_1 \sim \dots$  и  $B \sim B_1 \sim B_2 \sim \dots$  эквивалентных дивизоров. Если существуют такие целые  $j$  и  $k$ , что  $A_j = B_k$ , то, конечно,  $A \sim A_j = B_k \sim B$ . Обе последовательности  $A \sim A_1 \sim A_2 \sim \dots$ ,  $B \sim B_1 \sim B_2 \sim \dots$  в конце концов становятся периодическими, поэтому число дивизоров  $A_j$  и  $B_k$  конечно и условие  $A_j = B_k$  можно проверить вычислениями. Теорема, которую мы докажем в этом параграфе, утверждает, что достаточное условие  $A_j = B_k$

является также и необходимым, т. е. если  $A \sim B$ , то существуют такие целые  $j$  и  $k$ , что  $A_j = B_k$ ; здесь  $A \sim A_1 \sim A_2 \sim \dots$  и  $B \sim B_1 \sim B_2 \sim \dots$  — последовательности дивизоров, полученные применением циклического метода к  $A$  и  $B$ .

Условимся называть дивизор  $A_j$  *приведенным*, если применение к нему циклического метода в конце концов снова приводит к  $A_j$ . Тогда применение циклического метода к  $A_j$  дает нам конечный цикл приведенных эквивалентных дивизоров. Такой цикл называется *периодом* приведенных дивизоров. Применяя циклический метод к любому дивизору  $A$ , мы получаем период приведенных дивизоров, эквивалентных  $A$ . Аналогично, для любого данного  $B$  существует период приведенных дивизоров, эквивалентных  $B$ . Если  $A \sim B$ , то  $A_j \sim B_k$ , где  $A_j$  и  $B_k$  — приведенные дивизоры, эквивалентные  $A$  и  $B$  соответственно. Если мы применим циклический метод к  $A_j$ , то получим в точности те дивизоры, которые образуют период  $A_j$ ; то же самое можно сказать о  $B_k$ . Согласно теореме, которую мы собираемся доказать, из эквивалентности  $A_j$  и  $B_k$  следует, что какие-то два дивизора из этих периодов должны совпадать. Таким образом, сами эти периоды должны быть *идентичными*, т. е. должны состоять из одних и тех же дивизоров, расположенных в одном и том же циклическом порядке. Иначе говоря, из этой теоремы следует, что *два приведенных дивизора эквивалентны только тогда, когда их периоды совпадают*. Обратно, если этот факт известен и если  $A \sim B$ , то существуют приведенные дивизоры  $A_j \sim A$  и  $B_k \sim B$ , период  $A_j$  должен совпадать с периодом  $B_k$  и найдется такое  $i$ , что  $A_{j+i} = B_k$ , т. е. мы получаем отсюда теорему, которую собираемся доказать.

При  $D < 0$  последнее утверждение доказать легко. Рассмотрим сначала случай  $D < 0$ ,  $D \equiv 2$  или  $3 \pmod{4}$ . Пусть  $A$  и  $B$  — данные эквивалентные дивизоры:  $A \sim B$ . Не ограничивая общности, можно считать не только, что  $A$  и  $B$  приведены, но и что применение циклического метода как к  $A$ , так и к  $B$  увеличивает его норму. Из предположения  $A \sim B$  следует, что существует квадратичное целое  $x + y\sqrt{D}$  с дивизором  $A\bar{B}$ . Тогда  $x^2 - Dy^2 = ab$ , где  $a = N(A)$  и  $b = N(B)$ . Поскольку  $a \leq 2\sqrt{|D|/3}$  и  $b \leq 2\sqrt{|D|/3}$  (в противном случае следующий шаг циклического метода уменьшил бы норму), мы получаем, что  $x^2 - Dy^2 \leq 4|D|/3$ . Следовательно,  $y^2 = 0$  или  $1$ .

*Случай 1.* Если  $y^2 = 0$ , то  $A\bar{B}$  — дивизор целого  $x$ . В частности,  $x \equiv 0 \pmod{A}$ ,  $x \equiv 0 \pmod{a}$ ,  $x = ua$  для некоторого целого  $u$ . Аналогично,  $x = vb$  для некоторого  $v$ . Тогда  $ab = x^2 = uvab$ ,  $uv = 1$ ,  $u = v = \pm 1$ . Таким образом, числа  $a$ ,  $x$  и  $b$  имеют один и тот же дивизор; следовательно,  $A\bar{A} = A\bar{B} = B\bar{B}$  и  $A = B$ , что и требовалось доказать.

*Случай 2.* Если  $y^2 = 1$ , то либо  $x + y \sqrt{D}$ , либо  $-x - y \sqrt{D}$  имеет вид  $u - \sqrt{D}$  и его дивизором является  $A\bar{B}$ . Поскольку применение циклического метода к  $A$  дает  $r - \sqrt{D} \equiv 0 \pmod{A}$ , где  $|r|$  выбирается как можно меньшим, и  $a' = (r^2 - D)/a \geq a$ , мы получаем, что  $|r| \leq |u|$ ,  $b = (x^2 - D)/a = (u^2 - D)/a \geq \geq (r^2 - D)/a \geq a$ . Аналогично,  $a \geq b$ . Таким образом,  $a = b$ ,  $|u| = |r|$  и  $|u| = |r'|$ , где  $r' \equiv \sqrt{D} \pmod{B}$  с наименьшим возможным  $|r'|$ . Общее значение  $|r| = |u| = |r'|$  не превосходит  $a/2$ . Если оно равно  $a/2$ , то  $(r^2 - D)/a = a$  дает  $\frac{1}{4}a^2 - D = a^2$ ,  $D = -3(a/2)^2$ , где  $a$  четно. Поскольку  $D$  свободно от квадратов, отсюда следует, что  $a = 2$ ,  $D = -3$ , в противоречие предположению  $D \not\equiv 1 \pmod{4}$ . Таким образом,  $|r| = |r'| < a/2$ . Тогда из сравнения  $r \equiv u \equiv -r' \pmod{a}$  получаем, что  $r = -r'$ , и  $B$  следует за  $A$  в циклическом методе. Это завершает доказательство.

Доказательство в случае  $D < 0$ ,  $D \equiv 1 \pmod{4}$  является простой модификацией приведенного выше, и мы оставим его читателю (упр. 2). С другой стороны, при  $D > 0$  доказательство этой теоремы значительно сложнее<sup>1)</sup>. Рассмотрим сначала случай  $D > 0$ ,  $D \equiv 2$  или  $3 \pmod{4}$ . Мы должны доказать, что приведенные дивизоры  $A$  и  $B$ , принадлежащие различным периодам, не могут быть эквивалентными. Поэтому естественно начать доказательство с анализа понятия эквивалентности двух дивизоров.

Основная идея следующего доказательства — показать, что эквивалентность двух дивизоров  $A$  и  $B$  порождает целочисленную  $2 \times 2$ -матрицу, о которой в случае приведенных  $A$  и  $B$  известно достаточно, чтобы заключить, что она происходит из эквивалентности  $A$  с некоторым дивизором  $A$ , из его периода, полученного циклическим методом. Эквивалентность определяет  $2 \times 2$ -матрицу следующим образом.

Предположим, что  $A$  не делится ни на одно целое, большее 1. Тогда  $x + y \sqrt{D}$  делится на  $A$  в том и только в том случае, когда  $x + yr \equiv 0 \pmod{a}$ , где  $a = N(A)$  и  $r \equiv \sqrt{D} \pmod{A}$ . Другими словами,  $x + y \sqrt{D}$  делится на  $A$  тогда и только тогда, когда существуют такие целые  $u$  и  $v$ , что  $x + y \sqrt{D} = au + (r - \sqrt{D})v$ . Аналогично, если  $B$  не делится ни на одно целое, большее 1,

<sup>1)</sup> Доказательству этой теоремы Гаусс посвятил разд. 188—193 своих «Арифметических исследований». Он доказал несколько более общую теорему, но, как мы покажем в гл. 8, доказательство более общего случая не является более трудным. Дирихле называет эту теорему «самым трудным вопросом» теории ([D7, § 80]). Доказательство Дирихле, которое основывается на теории непрерывных дробей, внешне сильно отличается от приведенного здесь доказательства, но по существу они почти совпадают.

то квадратичное целое делится на  $B$  тогда и только тогда, когда оно имеет вид  $bu' + (s - \sqrt{D})v'$ , где  $b = N(B)$ ,  $s \equiv \sqrt{D} \pmod{B}$  и  $u', v'$  — целые. Если  $A$  и  $B$  — эквивалентные дивизоры, то существует квадратичное целое  $x + y\sqrt{D}$  с дивизором  $\bar{A}B$ . Умножение на  $x + y\sqrt{D}$  с последующим делением на  $a$  переводит квадратичные целые, делящиеся на  $A$ , в квадратичные целые, делящиеся на  $B$  (поскольку оно переводит квадратичное целое с дивизором  $AC$  в квадратичное целое с дивизором  $AC\bar{A}B/A\bar{A} = BC$ ). Если элементы из области определения этой операции записать в виде  $au + (r - \sqrt{D})v$ , а элементы из ее области значений — в виде  $bu' + (s - \sqrt{D})v'$ , то самой операции будет соответствовать целочисленная  $2 \times 2$ -матрица

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

Здесь для нахождения  $\alpha, \beta, \gamma, \delta$  положим сначала  $u = 1, v = 0$  и получим  $b\alpha + (s - \sqrt{D})\gamma = bu' + (s - \sqrt{D})v' = [a \cdot 1 + (r - \sqrt{D}) \times \times 0] (x + y\sqrt{D})/a = x + y\sqrt{D} = x + ys - y(s - \sqrt{D})$ ; отсюда  $\gamma = -y$ ,  $\alpha = (x + ys)/b$ . Положив затем  $u = 0, v = 1$ , найдем  $b\beta + (s - \sqrt{D})\delta = bu' + (s - \sqrt{D})v' = [a \cdot 0 + (r - \sqrt{D}) \cdot 1] \times \times (x + y\sqrt{D})/a = [(rx - yD) + (ry - x)\sqrt{D}]/a$  и получим отсюда  $\delta = (x - ry)/a$  и довольно сложное выражение для  $\beta$ , которое нам не потребуется в дальнейшем:  $\beta = (rx - yD - sx + rsy)/ab$ . Короче говоря, операция умножения на  $x + y\sqrt{D}$  с последующим делением на  $a$ , которая переводит квадратичные целые  $au + (r - \sqrt{D})v$  в квадратичные целые  $bu' + (s - \sqrt{D})v'$ , задается целочисленной  $2 \times 2$ -матрицей

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} \frac{x + ys}{b} & \frac{rx - yD - sx + rsy}{ab} \\ -y & \frac{x - yr}{a} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

Обратная к этой операция — умножение на  $x - y\sqrt{D}$  с последующим делением на  $b$  (поскольку  $(x + y\sqrt{D})(x - y\sqrt{D})/ab = 1$ ). Следовательно, матрица, обратная приведенной выше, равна

$$\begin{pmatrix} \frac{x - yr}{a} & \frac{sx + yD - rx - rsy}{ab} \\ y & \frac{x + ys}{b} \end{pmatrix}.$$

Действительно, она задает ту же операцию, что и выше, если поменять местами  $A$  и  $B$  и заменить  $x + y\sqrt{D}$  на  $x - y\sqrt{D}$ . В частности, это показывает, что обе матрицы имеют определитель 1.

В частном случае, когда  $A = A_0$  и  $B = A_1$  — дивизор, следующий за  $A_0$  в циклическом методе, имеем  $x + y \sqrt{D} = r_0 + \sqrt{D}$  и  $2 \times 2$ -матрица равна

$$\begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix},$$

где  $n_1 = (r_0 + r_1)/a_1$  и где элемент в верхнем правом углу не требует вычислений: действительно, он равен 1, поскольку вторая строка матрицы равна  $(-1, 0)$ , а ее определитель равен 1. Следовательно, операция, переводящая квадратичные целые, делящиеся на  $A_0$ , в квадратичные целые, делящиеся на  $A_j$ , и соответствующая цепочке эквивалентностей  $A_0 \sim A_1 \sim A_2 \sim \dots \sim A_j$ , задается  $2 \times 2$ -матрицей

$$\begin{pmatrix} n_j & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_{j-1} & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_2 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix}. \quad (1)$$

В частности, пусть  $E_A$  — матрица, которая получается, если в качестве  $j$  взять наименьшее положительное целое, для которого  $A_j = A_0$ . (Согласно предположению о приведенности  $A_0$ , такое  $j$  существует.) Если в явном виде задана эквивалентность  $A \sim B$ , соответствующая  $2 \times 2$ -матрице  $M$ , то матрица  $ME_A^n$  при всех положительных целых  $n$  также соответствует эквивалентности  $A \sim B$ . Доказательство будет заключаться в том, что мы покажем, что при достаточно большом  $n$  матрицу  $ME_A^n$  можно записать в виде (1); из единственности такого представления мы получим, что она действительно является матрицей (1) для некоторого  $j$  и, в частности, что  $B = A_j$  для некоторого  $j$ .

В качестве первого шага этой программы мы охарактеризуем матрицы вида (1). Важно заметить, что  $n_j$  — *знакопеременная последовательность*. Действительно,  $n_j = (r_{j+1} + r_j)/a_j$ ,  $r_j$  положительны (как было показано в § 7.5), а последовательность  $a_j$  — *знакопеременная* (поскольку  $a_j a_{j+1} = r_j^2 - D < 0$ ).

**Теорема.** Если целочисленная  $2 \times 2$ -матрица  $M$  имеет вид

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} = \pm \begin{pmatrix} n_j & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_{j-1} & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix}, \quad (2)$$

где  $n_1, n_2, \dots, n_j$  — *знакопеременная последовательность целых чисел*, то  $XW - YZ = 1$ ,  $|X| \geq |Z| \geq |W|$  и  $|X| \geq |Y| \geq |W|$ . Если некоторую матрицу можно записать в виде (2), то это можно сделать единственным способом, т. е.  $X, Y, Z$  и  $W$  однозначно определяют  $j$ , *знакопеременную последовательность*  $n_1, n_2, \dots, n_j$  и знак перед произведением. Наконец, три необходимых условия  $XW - YZ = 1$ ,  $|X| \geq |Z| \geq |W|$

$|X| \geq |Y| \geq |W|$  являются также и достаточными для того, чтобы матрица имела представление в виде (2).

**Доказательство.**  $XW - YZ = 1$ , поскольку определитель произведения равен произведению определителей. В дополнение к условиям  $|X| \geq |Z| \geq |W|$ ,  $|X| \geq |Y| \geq |W|$  будет показано, что знак <sup>1)</sup>  $XZ$  противоположен знаку  $n_j$ . Если  $j = 1$ , то очевидно, что все три условия выполняются. Предположим, что они выполняются при  $j - 1$  с некоторым  $j > 1$ . Тогда

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} = \begin{pmatrix} n_j & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} X' & Y' \\ Z' & W' \end{pmatrix}, \quad (3)$$

где  $|X'| \geq |Z'| \geq |W'|$ ,  $|X'| \geq |Y'| \geq |W'|$ , и знак  $X'Z'$  противоположен знаку  $n_{j-1}$ , т. е. совпадает со знаком  $n_j$ . Таким образом,  $X = n_j X' + Z'$ , где  $n_j X'Z' > 0$ ; поэтому два слагаемых  $n_j X'$  и  $Z'$  имеют одинаковый знак. Тогда  $|X| = |n_j| |X'| + |Z'| \geq |X'| = |-X'| = |Z'|$ . Знак  $XZ = (n_j X' + Z') \times \times (-X') = -n_j (X')^2 - X'Z'$  противоположен знаку  $n_j$ . Кроме того,  $Z = -X'$  и  $W = -Y'$ , так что  $|Z| \geq |W|$ . Остается показать, что  $|X| \geq |Y| \geq |W|$ . Из равенства  $X'W' - Y'Z' = 1$  следует, что  $X'W'Y'Z' = (Y'Z')^2 + (Y'Z')$  и  $X'W'Y'Z' \geq 0$ , поскольку  $x^2 + x \geq 0$  для всех целых  $x$ . Таким образом, либо  $W'Y' = 0$ , либо знак  $W'Y'$  совпадает со знаком  $X'Z'$  и  $n_j$ . Слагаемые в  $Y = n_j Y' + W'$  имеют одинаковые знаки и  $|Y| = |n_j| |Y'| + |W'| \geq |-Y'| = |W'|$ . Наконец,  $|Y| = |n_j| |Y'| + |W'| \leq |n_j| |X'| + |Z'| = |X|$ , и первое утверждение теоремы доказано.

Предположим теперь, что задано представление в виде (2). Тогда, как было только что показано, знак  $n_j$  определен тем, что он противоположен знаку  $XZ$ . Кроме того, равенство  $|X| = |n_j| |X'| + |Z'| = |n_j| |Z| + r$ , где  $0 \leq r \leq |Z|$ , показывает, что при  $r \neq 0$  или  $|Z|$  число  $|n_j|$  определяется однозначно как частное от деления  $|X|$  на  $|Z|$  с остатком. Если же  $r = 0$  или  $|Z|$ , то  $|Z|$  делит  $|X|$  без остатка, поэтому  $Z$  делит  $XW - YZ = 1$  и  $Z$  должно равняться  $\pm 1$ . Следовательно, если  $Z \neq \pm 1$ , то значение  $n_j$  можно определить по  $X$  и  $Z$  (хотя при этом нельзя определить значение  $j$ ). Затем уравнение (3) можно разрешить относительно  $X', Y', Z', W'$ , и этот процесс можно продолжить для нахождения  $n_{j-1}, n_{j-2}$  и т. д. до тех пор, пока не будет достигнуто  $Z = \pm 1$ . (Согласно принципу бесконечного спуска, значение  $Z = \pm 1$  должно достигаться, ибо  $r > 0$ ,  $|X| > |Z| = |X'|$ ,  $|X'| > |X''|$  и т. д.) Итак, доказательство единственности представления сводится к случаю  $Z = \pm 1$ .

<sup>1)</sup> В это утверждение включается утверждение о том, что  $XZ$  — число со знаком, т. е.  $X \neq 0$  и  $Z \neq 0$ .



Если  $Z = \pm 1$ , то  $W = 0$  или  $\pm 1$ , поскольку  $|W| \leq |Z|$ .

*Случай 1:*  $W = 0$ . В этом случае  $j$  должно быть равно 1, поскольку в противном случае существовало бы уравнение вида (3) и из  $W = 0$  следовало бы равенство  $-Y' = 0$ , что вместе с  $|Y'| \geq |W'|$  давало бы  $Y' = W' = 0$  — в противоречие с  $X'W' - Y'Z' = 1$ . Тогда знак перед правой частью (2) должен быть «—» при  $Z = 1$  и «+» при  $Z = -1$ . Таким образом,  $n_1 = n_j$  определяется из равенства  $X = \pm n_1$  (точнее,  $n_1 = -ZX$ ) и доказательство единственности завершено.

*Случай 2:*  $W = \pm 1$ . В этом случае  $j$  не может быть равно 1 и должно существовать равенство вида (3). Тогда из соотношений  $\pm 1 = Z = -X'$ ,  $|X'| \geq |Z'| \geq |W'|$  и  $|X'| \geq |Y'| \geq |W'|$  следует, что  $X' = \pm 1$ ,  $Y' = \pm 1$ ,  $Z' = \pm 1$  и  $W' = \pm 1$  или 0 (поскольку  $Y' \neq 0$  и  $Z' \neq 0$ ). Уравнение  $X'W' - Y'Z' = 1$  теперь показывает, что  $W'$  должно равняться нулю. Таким образом, равенство  $Y = n_j Y' + W' = n_j (-W)$  однозначно определяет  $n_j$  (и фактически определяет, что  $j = 2$ , поскольку  $W' = 0$ ), и доказательство единственности завершено.

Пусть теперь даны  $X, Y, Z, W$ , удовлетворяющие трем перечисленным выше условиям. Рассмотрим сначала исключительные случаи  $Z = \pm 1$ . Если  $W = 0$ , то  $-YZ = 1$ ,  $Y = -Z = \pm 1$  и сама матрица имеет требуемый вид. Если  $W = \pm 1$ , положим  $j = 2$ , найдем  $n_2$  из уравнения  $Y = -n_2 W$  и определим  $X', Y', Z', W'$  из (3). Тогда  $Y' = -W$ ,  $W' = 0$ ,  $Z' = -Y' = \pm 1$ , и, изменив, если понадобится, знаки в обеих частях (3), мы приведем его к виду

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} = \begin{pmatrix} n_2 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix},$$

который совпадает с требуемым видом (2), при условии что  $n_1$  и  $n_2$  имеют противоположные знаки. Так как  $Z = -n_1$  и  $Z = \pm 1$ , то  $n_1 = \pm 1$ . Таким образом,  $X = \pm |n_2| - 1$  и  $Y = n_2$ . Из неравенства  $|X| \geq |Y|$  следует, что  $X = -|n_2| - 1$ ,  $n_1 n_2 = -|n_2|$  и  $n_1, n_2$  имеют противоположные знаки. Наконец, рассмотрим случай  $|Z| > 1$ . Тогда  $|Z|$  не делит  $|X|$  нацело. Определим  $n_j$  (с неизвестным значением  $j$ ) из равенства  $|X| = |n_j| |Z| + r$ , где  $0 < r < |Z|$ , и из условия, что знак  $n_j$  противоположен знаку  $XZ$ . При таком определении  $n_j$  найдем  $X', Y', Z'$  и  $W'$  из (3). Тогда  $X = n_j X' + Z' = -n_j Z + Z'$ , и равенство  $|X| = |n_j| |Z| + r$  показывает, что знак  $Z'$  совпадает со знаком  $X$  и при этом  $|Z'| = r < |Z| = |X'|$ . Следовательно, знак  $X'Z' = (-Z) Z'$  совпадает со знаком  $-ZX$  и противоположен знаку  $XZ$ . Кроме того,  $X' = -Z$ ,  $Y' = -W$ , так что  $|X'| \geq |Y'|$ . Конечно,  $X'W' - Y'Z' = 1$ , поскольку произведение определителей равно определителю произведения:  $1 = XW - YZ = 1 \cdot (X'W' - Y'Z')$ . Теперь мы покажем, что  $|Y'| \geq$

$\geq |W'|$  и  $|Z'| \geq |W'|$ . Если  $|Z'| < |W'|$ , то  $|Y'| |Z'| + 1 \geq |Y'Z' + 1| = |X'W'| \geq |X'| (|Z'| + 1) = |X'| \times \times |Z'| + |X'| \geq |Y'| |Z'| + |X'|$ . Отсюда следует, что  $1 \geq \geq |X'| = |Z|$ , в противоречие предположению. Аналогично, если  $|Y'| < |W'|$ , то  $|Y'| |Z'| + 1 \geq |X'W'| \geq |X'| \times \times (|Y'| + 1) \geq |Z'| |Y'| + |X'|$ , поэтому  $1 \geq |X'| = |Z|$ . Это завершает доказательство того, что  $X', Y', Z', W'$  удовлетворяют трем условиям теоремы.

Таким образом, эти три условия гарантируют при  $Z \neq \pm 1$  существование равенства вида (3), в котором  $X', Y', Z', W'$  снова удовлетворяют трем условиям теоремы. Кроме того, знак  $n_j$  противоположен знаку  $XZ$  и совпадает со знаком  $X'Z'$ . Затем, если  $Z' \neq \pm 1$ , этот процесс можно повторить и отщепить новый множитель

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} = \begin{pmatrix} n_j & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_{j-1} & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} X'' & Y'' \\ Z'' & W'' \end{pmatrix}$$

(при этом значение  $j$  пока еще не определено), где  $n_j$  и  $n_{j-1}$  имеют противоположные знаки. Поскольку  $|Z| = |X'| > |Z'|$ , последовательность  $Z, Z', Z'', \dots$  убывает по абсолютной величине:  $|Z| > |Z'| > |Z''| > \dots$ . Согласно принципу бесконечного спуска, этот процесс должен закончиться и, поскольку  $|Z^{(m)}| \neq \neq 0$ , он должен закончиться при  $|Z^{(m)}| = 1$ . Тогда

$$\begin{pmatrix} X^{(m)} & Y^{(m)} \\ Z^{(m)} & W^{(m)} \end{pmatrix} = \pm \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix} \text{ или } \pm \begin{pmatrix} n_2 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix},$$

где знак  $n$  в крайнем слева множителе противоположен знаку  $X^{(m)}Z^{(m)}$ . Таким образом, мы получаем представление данной матрицы в требуемом виде, что завершает доказательство теоремы.

Итак, для того чтобы доказать, что при достаточно больших  $n$  матрица  $ME_A^n$  имеет требуемый вид, достаточно доказать, что при больших  $n$  она удовлетворяет трем условиям теоремы. Матрица  $E_A$  описывает отображение множества квадратичных целых, делящихся на  $A$ , в себя, заданное умножением на  $r_0 + \sqrt{D}$  с последующим делением на  $a_0$ , затем умножением результата на  $r_1 + \sqrt{D}$  с последующим делением на  $a_1$ , и т. д. Следовательно, это отображение соответствует просто умножению на единицу

$$\varepsilon_A = \frac{(r_0 + \sqrt{D})(r_1 + \sqrt{D}) \cdots (r_{j-1} + \sqrt{D})}{a_0 a_1 \cdots a_{j-1}}$$

(как числитель, так и знаменатель имеют дивизор  $A_0 \bar{A}_1 A_1 \bar{A}_2 \dots \dots \bar{A}_{j-1} A_{j-1} \bar{A}_0$ , поскольку  $A_j = A_0$ ). Таким образом, матрица  $ME_A^n$  соответствует умножению на  $(x + y \sqrt{D}) \varepsilon_A^n$  с последующим

делением на  $a$ , где  $x + y \sqrt{D}$  — данное квадратичное целое с дивизором  $\bar{A}B$ . Это показывает, что матрица  $ME_A^n$  является просто новой матрицей  $M$ , которая получается, если  $x + y \sqrt{D}$  заменить на квадратичное целое  $(x + y \sqrt{D}) \varepsilon_A^n$  с тем же самым дивизором  $\bar{A}B$ . Так мы приходим к вопросу о нахождении условий для  $x$  и  $y$ , при которых матрица

$$M = \begin{pmatrix} \frac{x+ys}{b} & \frac{rx-yD-sx+rsy}{ab} \\ -y & \frac{x-yr}{a} \end{pmatrix}$$

удовлетворяет условиям теоремы. Поскольку определитель  $M$  равен 1, этот вопрос сводится к нахождению условий, при которых выполняются неравенства  $|X| \geq |Y| \geq |W|$ ,  $|X| \geq |Z| \geq |W|$ .

Коэффициенты в  $\varepsilon_A$  имеют одинаковые знаки, поэтому, как видно из доказательства в § 7.5, считая  $n$  большим, мы можем предположить, что  $x$  и  $y$  велики по абсолютной величине и имеют одинаковые знаки. Тогда из  $x^2 - Dy^2 = ab$ ,  $x^2 = ab + (D - r^2)y^2 + r^2y^2$ , где  $ab$  фиксировано и  $D - r^2 > 0$ , следует, что  $x^2 > r^2y^2$  (при достаточно большом  $|y|$ ) и  $|x| > |r||y|$ ,  $|x - ry| = |x| - r|y|$  (если  $x$  и  $y$  имеют одинаковые знаки). Таким образом, неравенство  $|Z| > |W|$  равносильно неравенству  $|a||y| > |x| - r|y|$ , которое в свою очередь эквивалентно  $(r + |a|) \times |y| > |x|$ ,  $y^2(r + |a|)^2 > x^2 = ab + Dy^2$ . Последнее неравенство выполняется при больших  $|y|$ , поскольку  $(r + |a|)^2 > D$  (в противном случае  $r$  можно было бы увеличить). Аналогично,  $|x + ys| = |x| + s|y|$ , если  $x$  и  $y$  имеют одинаковые знаки, и неравенство  $|X| > |Z|$  эквивалентно неравенству  $|x| + s|y| > |b||y|$ , или  $|x| > (-s + |b|)|y|$ . Конечно, если  $-s + |b| \leq 0$ , то последнее неравенство выполняется. В противном случае оно эквивалентно неравенству  $x^2 > (-s + |b|)^2 y^2$ , или неравенству  $ab + Dy^2 > (s - |b|)^2 y^2$ ; последнее справедливо при больших  $|y|$ , поскольку  $(s - |b|)^2 < D$  (см. § 7.5, где было показано, что если  $a_{j+1} < 0$ , то  $(r_{j+1} + a_{j+1})^2 < D$ , но если  $a_{j+1} > 0$ , то  $(r_{j+1} - a_{j+1})^2 < D$ ). Следовательно,  $|X| > |Z| > |W|$ , если  $|y|$  достаточно велико и если  $x$  и  $y$  имеют одинаковые знаки. Тогда  $|Y||Z| = |XW - 1| \geq |X| \times |W| - 1 > |Z||W| - 1$ , если  $|W| \neq 0$  (при  $|W| = 0$  неравенство  $|Y| \geq |W|$  очевидно). Отсюда следует, что  $|Y||Z| \geq |W||Z|$  и  $|Y| \geq |Z|$  (поскольку  $|Z| > |W| \geq 0$ ). Аналогично,  $|Y||Z| \leq |X||W| + 1 < |X||Z| + 1$ ,  $|Y| \leq |X|$ , причем все неравенства доказаны при большом  $|y|$  и  $xy > 0$ .

Итак, если  $A$  и  $B$  приведены и  $A \sim B$ , то, не ограничивая общности, можно предположить, что эквивалентность между ними соответствует матрице  $M$  изученного в теореме типа. В этом доказательстве используется лишь то свойство  $\varepsilon_A$ , что это единица с коэффициентами одного знака. Следовательно, оно показывает, что эквивалентность  $B \sim B$ , соответствующая квадратичному целому  $b\varepsilon_A^n$  с дивизором  $BB$ , определяет матрицу  $M_B$ , которая также имеет вид, изученный в теореме, по крайней мере для больших  $n$ . (В действительности достаточно велико уже  $n = 1$ . См. упр. 6.)

Далее,  $M_B M = M E_A^n$ , поскольку каждая из этих матриц описывает отображение множества квадратичных целых, делящихся на  $A$ , в множество квадратичных целых, делящихся на  $B$ , которое получается умножением на  $(x + y \sqrt{D}) \varepsilon_A^n$  с последующим делением на  $a$ . (В левой части происходит сокращение одного множителя  $a$  в числителе и знаменателе, в правой части сокращаются  $n$  множителей  $a$  в числителе и в знаменателе.) Каждая из матриц  $M_B$ ,  $M$  и  $E_A$  имеет вид

$$\pm \Pi \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix},$$

где числа  $n$  образуют знакочередующуюся последовательность целых. Кроме того,  $M_B M$  и  $M E_A^n$  тоже имеют такой вид, и их разложения в этом виде получаются просто перемножением разложений их сомножителей. Для того чтобы доказать это утверждение, необходимо показать, что знак  $n$  в крайнем справа множителе в  $M_B$  противоположен знаку  $n$  в крайнем слева множителе  $M$ ; аналогичными свойствами обладают крайний справа множитель  $M$  и концевые множители  $E_A$ . Поскольку, согласно определению,  $E_A$  имеет четное число множителей, числа  $n$  входят в его два крайних множителя с противоположными знаками. В крайний справа множитель входит  $(r_0 + r_1)/a_0$ , знак которого совпадает со знаком  $a_0 = N(A)$ . Следовательно, знак  $n$  в крайнем слева множителе противоположен знаку  $N(A)$ . Число  $n$  в крайнем слева множителе  $M$  имеет знак, противоположный знаку  $XZ = -(x + ys)y/b$ . Поскольку  $x$  и  $y$  имеют одинаковые знаки, отсюда следует, что рассматриваемый знак совпадает со знаком  $N(B)$ . Число  $n$  в крайнем справа множителе  $M$  имеет знак, совпадающий со знаком  $XY$  (упр. 3). Так как  $XYZW = (YZ - 1)YZ \geq 0$  и  $W \neq 0$ , то этот знак совпадает со знаком  $ZW = -y(x - yr)/a$ . Следовательно, знак  $n$  в крайнем справа множителе  $M$  противоположен знаку  $n$  в крайнем слева множителе  $E_A$ . Знаки концевых множителей  $M_B$  можно найти аналогичным образом. Тогда  $M_B^k M = M E_A^{nk}$  для всех  $k$  является разложением рассматриваемого в теореме типа, и из утверждения этой теоремы о един-

ственности следует, что множители в разложении  $M$  равны последним множителям в  $E_A^{nk}$  для достаточно больших  $k$ , т. е. что для некоторого  $j$

$$\pm M = \begin{pmatrix} n_j & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_{j-1} & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix},$$

где  $n_1, n_2, \dots$  — циклически повторяющаяся последовательность, полученная применением циклического метода к  $A$ . Следовательно, матрица, соответствующая эквивалентности  $A \sim B$ , совпадает с матрицей, соответствующей эквивалентности  $A \sim A_j$ , которая получается из подходящего количества циклов по периоду  $A$ .

Матрица  $M$  возникает, с одной стороны, при умножении на  $x + y \sqrt{D}$ , имеющее дивизор  $\bar{A}B$ , с последующим делением на  $a$ , а с другой стороны, при умножении на некоторое  $x' + y' \sqrt{D}$ , имеющее дивизор  $\bar{A}A_j$ , с последующим делением на  $a$ . Значения  $x$  и  $y$  однозначно определяются матрицей  $M$  и дивизором  $A$ . Действительно, последняя строка  $M$  равна  $-y, (x - yr)/a$ , откуда при известных  $a$  и  $r$  легко получаются  $x$  и  $y$ . Следовательно,  $x = x', y = y'$  и  $\bar{A}B = \bar{A}A_j$ . Это показывает, что  $B = A_j$ , и завершает доказательство в случае  $D > 0, D \equiv 2$  или  $3 \pmod{4}$ .

При  $D > 0, D \equiv 1 \pmod{4}$  требуются лишь незначительные изменения. Квадратичные целые, делящиеся на  $A$ , имеют вид  $au + (r - \frac{1}{2}\sqrt{D})v$  с целыми  $u$  и  $v$ . Эквивалентность между двумя дивизорами  $A \sim B$  соответствует целочисленной  $2 \times 2$ -матрице, а именно

$$\begin{pmatrix} \frac{x+2ys}{b} & \frac{rx - \frac{1}{2}yD - sx + 2rsy}{ab} \\ -2y & \frac{x - 2yr}{a} \end{pmatrix},$$

где  $x + y \sqrt{D}$  имеет дивизор  $\bar{A}B$ . (Здесь  $x$  и  $y$  могут одновременно быть целыми или полуцелыми, однако элементы приведенной выше матрицы всегда будут целыми.) Остальная часть доказательства проходит так же, как и раньше.

## Упражнения

1. Докажите, что если  $D \equiv 2$  или  $3 \pmod{4}$  и  $A, B$  — дивизоры с равными нормами, которые делят  $r - \sqrt{D}$ , то  $A = B$ . [По существу, это означает, что дивизор однозначно определяется множеством объектов, которые он делит. Как видно из § 7.3, при  $D > 0$  это утверждение неверно. Однако справедливо утверждение о том, что если  $A$  и  $B$  делят в точности одни и те же квадратичные целые, то либо  $A = B$ , либо  $A = (-1, *)B$ .]

2. Докажите теорему о том, что эквивалентные дивизоры соответствуют одним и тем же периодам при  $D \equiv 1 \pmod{4}, D < 0$ .

3. Докажите, что знак  $n_0$  в (2) совпадает со знаком  $XY$ . [Это можно сделать либо простой индукцией, либо используя тот факт, что  $n_j$  имеет знак  $-XZ$ , и рассматривая транспонированную матрицу.]

4. Сформулируйте и докажите теорему, аналогичную приведенной в тексте, о разложении вида

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} = \begin{pmatrix} n_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} n_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_1 & 1 \\ 1 & 0 \end{pmatrix} \quad (4)$$

с положительными  $n_j$ . По существу, здесь к  $X$  и  $Z$  применяется алгоритм Евклида, и доказать эту теорему намного легче, чем теорему из основного текста.

5. Докажите, что разложение вида (2) всегда можно получить из разложения вида (4), соответствующим образом введя в него знаки (и тем самым получите новое доказательство приведенной в тексте теоремы).

6. Пусть  $\varepsilon_D = u + v\sqrt{D}$  — единица с  $u$  и  $v$  одного знака. Предположим, что  $B$  — приведенный дивизор, а  $M_B$  есть  $2 \times 2$ -матрица, соответствующая отображению множества квадратичных целых, делящихся на  $B$ , в себя, полученному умножением на квадратичное целое  $b\varepsilon_D$  с дивизором  $B\bar{B}$ . Докажите, что тогда к матрице  $M_B$  применима теорема этого параграфа.

## 7.8. Теоремы Эйлера

Проводя вычисления в теории дивизоров квадратичных целых, мы должны установить, какие простые распадаются, какие остаются простыми и какие разветвляются. По существу, это сводится к задаче определения для данного свободного от квадратов  $D$  и данного нечетного простого  $p$ , не делящего  $D$ , имеет ли решение сравнение  $D \equiv x^2 \pmod{p}$ . Конечно, на этот вопрос можно ответить, если найти все квадраты по модулю  $p$  (в количестве  $(p-1)/2$ ) и проверить, содержится ли среди них  $D$ . Однако при решении этой задачи обнаруживаются странные и удивительные закономерности; Эйлер заметил их (и опубликовал соответствующие результаты) более чем за столетие до того, как появилась теория идеального разложения Куммера. Этот параграф посвящен описанию закономерностей, найденных Эйлером.

Эйлер почти буквально *открыл* эти закономерности эмпирически — внимательно изучая числовые примеры. Он сформулировал эти теоремы уже в сороковые годы XVIII века (см. [E7] и [F6, стр. 146—151]) — в довольно ранний период своей деятельности, — но так и не смог впоследствии доказать <sup>1)</sup> их. Как заметил Гаусс (Disquisitiones Arithmeticae, Art. 151), из теорем Эйлера <sup>2)</sup> сле-

<sup>1)</sup> Смит [S3, разд. 16] пишет: «... его [Эйлера] заключения основываются только на индукции [т. е. эмпирическом наблюдении], хотя в одном мемуаре Эйлер, по-видимому, вообразил (здесь он недостаточно ясно выразил свои мысли), что им получено удовлетворительное доказательство этих теорем». Однако в другом месте — в статье, опубликованной в конце жизни, — «Эйлер явно замечает, что эта теорема осталась недоказанной». Изучающие Эйлера, должно быть, привыкли к таким парадоксам.

<sup>2)</sup> Кажется, историки часто не замечают признания Гауссом того факта, что Эйлер сформулировал теоремы, из которых следует квадратичный закон



дует квадратичный закон взаимности, и наоборот, из квадратичного закона взаимности можно вывести эти результаты Эйлера. Таким образом, поскольку Гаусс дал первое доказательство квадратичного закона взаимности, то заслуга первого доказательства этих теорем также принадлежит Гауссу.

Задача, которую изучал Эйлер, состояла в том, может ли данное простое делить число вида  $x^2 + ny^2$ , где  $n$  — данное целое, а  $x$  и  $y$  — взаимно простые целые числа. Суть его открытия состоит в удивительном наблюдении, что *ответ на этот вопрос зависит только от класса вычетов данного простого по модулю  $4n$* . То есть если  $p_1$  и  $p_2$  — простые, сравнимые по модулю  $4n$ , то взаимно простые целые  $x_1$  и  $y_1$ , такие, что  $p_1 \mid x_1^2 + ny_1^2$ , существуют тогда и только тогда, когда существуют такие взаимно простые  $x_2, y_2$ , что  $p_2 \mid x_2^2 + ny_2^2$ .

Для того чтобы сформулировать это утверждение в терминологии данной главы, естественно положить  $n = -D$ , так что  $x^2 + ny^2$  становится нормой  $x + y\sqrt{D}$ . Мы будем рассматривать только случай свободного от квадратов  $D$ . (Как показывают упр. 1 и 9, это не приводит к реальной потере общности.) Если  $p$  делит  $4D$ , то теорема Эйлера ничего не говорит о нем, поскольку такое  $p$  не сравнимо ни с одним простым по модулю  $4D$ . Следовательно, в тех случаях, когда выполняются условия теоремы,  $p$  не разветвляется и либо распадается, либо остается простым. Если  $p$  распадается, то сравнение  $D \equiv x^2 \pmod{p}$  имеет ненулевое решение  $x$ ,  $p \mid x^2 - D \cdot 1^2$ , и теорема Эйлера утверждает, что при  $p_1 \equiv \equiv p \pmod{4D}$  существуют такие взаимно простые  $x_1, y_1$ , для которых  $p_1 \mid x_1^2 - Dy_1^2$ . Отсюда следует, что  $p_1$  делит  $(x_1 - y_1\sqrt{D}) \times$

---

взаимности. Гаусс признает за собой лишь приоритет формулировки квадратичного закона взаимности в простом виде: «если  $p \equiv 1 \pmod{4}$ , то  $q$  является квадратом по модулю  $p$  тогда и только тогда, когда  $p$  является квадратом по модулю  $q$ , и если  $p \equiv -1 \pmod{4}$ , то  $q$  является квадратом по модулю  $p$  тогда и только тогда, когда  $-p$  является квадратом по модулю  $q$ ». Впоследствии Гаусс, кажется, решил, что, приписывая себе приоритет этой формулировки, он допускает несправедливость по отношению к Лежандру. Действительно, всего через несколько лет он пишет [G3]: «Конечно, мы должны считать Лежандра первооткрывателем этой в высшей степени элегантной теоремы». И в самом деле, формулировка Лежандра квадратичного закона взаимности, согласно которой  $p$  является квадратом по модулю  $q$  тогда и только тогда, когда  $q$  является квадратом по модулю  $p$ , за исключением случая  $p \equiv q \equiv \equiv -1 \pmod{4}$ , в котором  $p$  является квадратом по модулю  $q$  тогда и только тогда, когда  $q$  не является квадратом по модулю  $p$ , — кажется даже проще формулировки Гаусса. Самой ясной формулировкой Эйлера этого закона обычно считается формулировка в [E11], которая, конечно, менее проста, чем формулировка Гаусса или Лежандра. (В английском переводе «Арифметических исследований» допущены слишком большие вольности в обращении с текстом разд. 151, в результате чего в нем отсутствует то место, в котором Гаусс признает заслуги Эйлера. По этому вопросу следует обратиться к тексту оригинала или других переводов.)

$\times (x_1 + y_1 \sqrt{D})$ , но не делит ни один из сомножителей (так как  $x_1$  и  $y_1$  взаимно просты, то ни одно целое, за исключением, возможно, 2, не делит оба сомножителя одновременно). Таким образом, поскольку  $p_1$  не разветвляется, оно должно распадаться. Короче говоря, из теоремы Эйлера следует, что *если  $p_0 \equiv p_1 \pmod{4D}$ , то  $p_1$  распадается, разветвляется или остается простым тогда и только тогда, когда  $p_0$  распадается, разветвляется или остается простым соответственно*<sup>1)</sup>. Легко показать (упр. 1), что и обратно, из последней теоремы следует теорема Эйлера. Поэтому последнее утверждение разумно рассматривать как *переформулировку* теоремы Эйлера в терминах теории дивизоров квадратичных целых.

Эта теорема (если предположить, что она справедлива) позволяет определить, каким образом простые  $p$  разлагаются в квадратичных целых  $x + y \sqrt{D}$ . Кроме простых делителей числа  $4D$  необходимо проверить только одно простое из каждого<sup>2)</sup> класса вычетов по модулю  $4D$ , взаимно простого с  $4D$ . Например, при  $D = 2$  из того факта, что простые 3 и 5 остаются простыми (квадраты по модулю 3 сравнимы с  $1 \not\equiv 2 \pmod{3}$ , а по модулю 5 сравнимы с 1,  $4 \not\equiv 2 \pmod{5}$ ), мы получаем, согласно нашей теореме, что все простые  $\equiv 3$  или  $5 \pmod{8}$  остаются простыми, а из того, что 17 и 7 распадаются ( $6^2 \equiv 2 \pmod{17}$ ,  $3^2 \equiv 2 \pmod{7}$ ), следует, что все простые  $\equiv 1$  или  $7 \pmod{8}$  распадаются. Единственное оставшееся простое 2 разветвляется.

Таким образом, на основании этой теоремы мы можем определить закономерности разложения простых для различных значений  $D$ . Некоторые результаты (значительно менее обширные, чем вычисления Эйлера) приведены в табл. 7.8.1. Из этой таблицы следует очевидное заключение: *в точности половина классов простых по модулю  $4D$  являются распадающимися*<sup>3)</sup> *классами*, т. е.

<sup>1)</sup> Аналогичное явление наблюдалось и в случае круговых целых, где число простых дивизоров, делящих  $p$ , зависит только от показателя  $p$  по модулю  $\lambda$  и, следовательно, только от класса вычетов  $p$  по модулю  $\lambda$ . В случае алгебраических целых, более общих, чем квадратичные или круговые целые, это явление обычно *не* встречается, т. е. не так легко предсказать способ разложения простых  $p$ . Законы взаимности и теория полей классов тесно связаны с этим особым свойством квадратичных и круговых целых.

<sup>2)</sup> В частных случаях, конечно, мы обнаружим, что каждый класс, взаимно простой с  $4D$ , содержит простое. Действительно, согласно знаменитой теореме Дирихле, каждый класс, взаимно простой с любым модулем  $m$  (в данном случае  $m = 4D$ ), содержит бесконечно много простых чисел (см. § 9.7).

<sup>3)</sup> Для того чтобы избежать неявного обращения к упомянутой в предыдущем примечании теореме Дирихле, лучше сформулировать данную теорему в следующем виде: классы по модулю  $4D$ , взаимно простые с  $4D$ , можно разбить на два подмножества с одинаковым числом элементов, называемых *распадающимися классами* и *нераспадающимися классами*, таким образом, что любое простое в распадающемся классе распадается, а любое простое в нерас-

**Таблица 7.8.1.** Числа, напечатанные жирным шрифтом, принадлежат распадающимся классам, т. е. любое простое, сравнимое по модулю  $4D$  с таким числом, распадается в квадратичных целых детерминанта  $D$

$D = -1$	<b>1</b>	<b>3</b>															
$D = -2$	<b>1</b>	<b>3</b>	<b>5</b>	<b>7</b>													
$D = -3$	<b>1</b>	<b>5</b>	<b>7</b>	<b>11</b>													
$D = -5$	<b>1</b>	<b>3</b>	<b>7</b>	<b>9</b>	<b>11</b>	<b>13</b>	<b>17</b>	<b>19</b>									
$D = -6$	<b>1</b>	<b>5</b>	<b>7</b>	<b>11</b>	<b>13</b>	<b>17</b>	<b>19</b>	<b>23</b>									
$D = -7$	<b>1</b>	<b>3</b>	<b>5</b>	<b>9</b>	<b>11</b>	<b>13</b>	<b>15</b>	<b>17</b>	<b>19</b>	<b>23</b>	<b>25</b>	<b>27</b>					
$D = -10$	<b>1</b>	<b>3</b>	<b>7</b>	<b>9</b>	<b>11</b>	<b>13</b>	<b>17</b>	<b>19</b>	<b>21</b>	<b>23</b>	<b>27</b>	<b>29</b>	<b>31</b>	<b>33</b>	<b>37</b>	<b>39</b>	
$D = 2$	<b>1</b>	<b>3</b>	<b>5</b>	<b>7</b>													
$D = 3$	<b>1</b>	<b>5</b>	<b>7</b>	<b>11</b>													
$D = 5$	<b>1</b>	<b>3</b>	<b>7</b>	<b>9</b>	<b>11</b>	<b>13</b>	<b>17</b>	<b>19</b>									
$D = 6$	<b>1</b>	<b>5</b>	<b>7</b>	<b>11</b>	<b>13</b>	<b>17</b>	<b>19</b>	<b>23</b>									
$D = 7$	<b>1</b>	<b>3</b>	<b>5</b>	<b>9</b>	<b>11</b>	<b>13</b>	<b>15</b>	<b>17</b>	<b>19</b>	<b>23</b>	<b>25</b>	<b>27</b>					
$D = 10$	<b>1</b>	<b>3</b>	<b>7</b>	<b>9</b>	<b>11</b>	<b>13</b>	<b>17</b>	<b>19</b>	<b>21</b>	<b>23</b>	<b>27</b>	<b>29</b>	<b>31</b>	<b>33</b>	<b>37</b>	<b>39</b>	

содержат распадающиеся простые. Далее, менее очевидный факт, замеченный Эйлером, состоит в том, что *произведение распадающихся классов является распадающимся классом*; здесь умножением является обычное умножение целых по модулю  $4D$ . С этими двумя замечаниями тесно связано (а в действительности является их следствием <sup>1)</sup>) утверждение, что *квадрат любого класса, взаимно простого с  $4D$ , является распадающимся классом*.

Заключительное замечание, которое совершенно очевидно из таблицы и которое Эйлер, конечно, сделал, состоит в том, что *при  $D > 0$  класс, противоположный распадающемуся, является распадающимся; если же  $D < 0$ , то класс, противоположный распадающемуся, является нераспадающимся*. Поскольку переход к противоположному является взаимно однозначным соответствием и поскольку половина классов распадающиеся, эти утверждения равносильны обратным к ним, т. е. равносильны тому, что *при  $D > 0$  класс, противоположный нераспадающемуся, является нераспадающимся, а при  $D < 0$  класс, противоположный нераспадающемуся, является распадающимся*.

Эти теоремы значительно облегчают нахождение распадающихся классов. Например, при  $D = 2$  класс 1 должен быть распадаю-

падающемся классе остается простым. Формулировки других теорем также следует немного изменить, допустив существование классов, которые не содержат простых и, следовательно, не являются ни распадающимися, ни нераспадающимися. Мы предоставляем читателю сделать эти изменения, предусматривающие ситуацию, которая никогда не возникает.

<sup>1)</sup> См. упр. 6.

щимся, так как он является квадратом. Поскольку  $D > 0$ , отсюда следует, что класс  $-1$  также должен быть распадающимся. Остальные классы — классы  $\pm 3$  — должны быть нераспадающимися, так как распадающимися могут быть только половина всех классов. В качестве другого примера рассмотрим случай  $D = -11$ . Здесь класс 3 является распадающимся, поскольку  $-11 \equiv 1^2 \pmod{3}$ . Следовательно, все классы  $1, 3, 3^2, 3^3 \equiv -17, 3^4 \equiv -7, 3^5 \equiv -21, 3^6 \equiv -19, 3^7 \equiv -13, 3^8 \equiv 5, 3^9 \equiv 15, 3^{10} \equiv 1 \pmod{44}$  являются распадающимися. Поскольку они составляют половину из 20 классов, взаимно простых с 44, остальные классы будут нераспадающимися. Заметим, что они противоположны распадающимся классам.

В качестве третьего примера рассмотрим случай  $D = -15$ . Здесь наименьшим простым, подлежащим рассмотрению, является  $p = 7$ . Поскольку  $-15 \equiv -1$  не является квадратом по модулю 7 (1, 2 и 4 — все квадраты по модулю 7), класс 7 — нераспадающийся. Следовательно, класс  $-7$  — распадающийся, и такими же являются классы  $(-7)^2 \equiv -11, (-7)^3 \equiv 17$  и  $(-7)^4 \equiv 1 \pmod{60}$ . Это дает 4 из 8 распадающихся классов. В точности один из классов  $\pm 13$  является распадающимся, но мы еще пока не определили, какой именно. Квадраты по модулю 13 исчерпываются классами 1, 4,  $-4, 3, -1, -3$ , и в их число не входит класс  $-15 \equiv -2 \pmod{13}$ . Следовательно, 13 является нераспадающимся классом, а  $-13$  — распадающимся. Тогда  $(-13)^2 \equiv -11, (-13)^3 \equiv 23, (-13)^4 \equiv (-7)^4 \equiv 1 \pmod{60}$  также являются нераспадающимися классами, что дает нам еще 2 распадающихся класса. Кроме того,  $(-7)(-13) \equiv -29$  и  $(-7)^3(-13) \equiv 17(-13) \equiv 19$  также будут распадающимися классами. Таким образом, распадающимися классами будут классы 1,  $-7, -11, -13, 17, 19, 23, -29$ , а нераспадающимися — противоположные к ним.

Все эти теоремы Эйлера легко вывести из квадратичного закона взаимности (см. § 5.6 или данное ниже примечание). Первая теорема, которая является главной, состоит просто в том, что значение символа Лежандра <sup>1)</sup>  $\left(\frac{D}{p}\right)$  при нечетных простых  $p \nmid D$  зависит только от класса  $p$  по модулю  $4D$ . Это утверждение будет

---

<sup>1)</sup> Символ Лежандра  $\left(\frac{n}{p}\right)$  определен в § 5.6. Он имеет смысл только тогда, когда  $p$  — нечетное простое, а  $n$  — целое, не делящееся на  $p$ , и равен  $+1$ , если  $n$  является квадратом по модулю  $p$  (сравнение  $n \equiv x^2 \pmod{p}$  имеет решение), и  $-1$  в противном случае. Легко показать, что если ни  $n_1$ , ни  $n_2$  не делятся на  $p$ , то  $\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right) \left(\frac{n_2}{p}\right)$ . Квадратичный закон взаимности утверждает, что если  $p$  и  $q$  — нечетные простые и если  $p \equiv 1 \pmod{4}$ , то  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ , тогда как при  $p \equiv 3 \pmod{4}$  имеем  $\left(\frac{-p}{q}\right) = \left(\frac{q}{p}\right)$ . Дополнительные законы взаимности утверждают, что  $\left(\frac{-1}{p}\right) \equiv p \pmod{4}$ , т. е.  $\left(\frac{-1}{p}\right) = 1$ , если  $p \equiv 1 \pmod{4}$ , и  $-1$ , если  $p \equiv -1 \pmod{4}$ , и что  $\left(\frac{2}{p}\right)$  равно  $+1$ , если  $p \equiv \pm 1 \pmod{8}$ , и  $-1$ , если  $p \equiv \pm 3 \pmod{8}$ .

доказано, если показать, как применение квадратичного закона взаимности позволяет *вычислить*  $\left(\frac{D}{p}\right)$  при помощи только класса  $p$  по модулю  $4D$ . Для этого предположим, что  $D$  записано в виде произведения чисел, для которых квадратичный закон взаимности имеет простой вид, а именно чисел  $-1$ , или  $2$ , или  $p$ , где  $p \equiv 1 \pmod{4}$ , или  $-p$ , где  $p \equiv -1 \pmod{4}$ . То есть пусть  $D = \varepsilon r p_1 p_2 \dots p_\mu (-p'_1) (-p'_2) \dots (-p'_\nu)$ , где  $\varepsilon = \pm 1$ ,  $r = 1$  или  $2$ ,  $p_i$  — простое, сравнимое с  $1$  по модулю  $4$ , и  $p'_i$  — простое, сравнимое с  $-1$  по модулю  $4$ . Тогда, согласно квадратичному закону взаимности,

$$\begin{aligned} \left(\frac{D}{p}\right) &= \left(\frac{\varepsilon}{p}\right) \left(\frac{r}{p}\right) \left(\frac{p_1}{p}\right) \dots \left(\frac{p_\mu}{p}\right) \left(\frac{-p'_1}{p}\right) \dots \left(\frac{-p'_\nu}{p}\right) = \\ &= \left(\frac{\varepsilon}{p}\right) \left(\frac{r}{p}\right) \left(\frac{p}{p_1}\right) \dots \left(\frac{p}{p_\mu}\right) \left(\frac{p}{p'_1}\right) \dots \left(\frac{p}{p'_\nu}\right) \end{aligned}$$

(где  $\left(\frac{1}{p}\right)$  считается равным  $+1$  при всех  $p$ , если  $\varepsilon$  или  $r$  равно  $1$ ). Первый множитель в правой части зависит только от класса  $p$  по модулю  $4$  и, следовательно, только от класса  $p$  по модулю  $4D$ . Вторым множителем равен  $+1$ , если  $r \neq 2$ ; при  $r = 2$  он зависит только от класса  $p$  по модулю  $8$ . Из  $r = 2$  следует, что  $D$  четно, поэтому класс  $p$  по модулю  $4D$  однозначно определяет класс  $p$  по модулю  $8$ , а тем самым и второй знак  $\left(\frac{r}{p}\right)$ . Остальные знаки зависят только от класса  $p$  по модулю  $p_i$  или  $p'_i$  и, следовательно, только от класса  $p$  по модулю  $4D$ . Это завершает доказательство того, что  $\left(\frac{D}{p}\right)$  зависит только от класса  $p$  по модулю  $4D$ .

Это доказательство дает в действительности больше, поскольку оно показывает, как определение символа  $\left(\frac{D}{p}\right)$  можно *распространить* с нечетных простых  $p$ , которые не делят  $D$ , на все целые  $p$ , взаимно простые с  $2D$  (и даже, при  $\varepsilon = r = 1$ , на все целые, взаимно простые с  $D$ ). Это расширенное определение  $\left(\frac{D}{n}\right)$  для  $n$ , взаимно простых с  $4D$ , называется *символом Якоби*<sup>1)</sup>. Класс  $n$  является распадающимся, если  $\left(\frac{D}{n}\right) = +1$ , и нераспадающимся, если  $\left(\frac{D}{n}\right) = -1$ . Это определение распадающихся и нераспадающихся классов не предполагает, что класс  $n$  содержит простое, и, следовательно, не опирается на теорему Дирихле о простых в арифметической прогрессии.

Из определения символа Якоби ясно, что  $\left(\frac{D}{n_1 n_2}\right) = \left(\frac{D}{n_1}\right) \left(\frac{D}{n_2}\right)$ . Действительно, это равенство справедливо для каждого из сомножителей. Следовательно, не только произведение двух распадаю-

<sup>1)</sup> См. Якоби [J1]; там  $\left(\frac{D}{n}\right)$  определено для нечетных  $n$ , взаимно простых с  $D$ , как  $\left(\frac{D}{p_1}\right) \left(\frac{D}{p_2}\right) \dots \left(\frac{D}{p_\nu}\right)$ , где  $n = p_1 p_2 \dots p_\nu$  — разложение  $n$  на простые множители. Легко видеть, что это эквивалентно приведенному выше определению.



щихся классов, но и произведение двух нераспадающихся классов является распадающимся классом, а произведение нераспадающегося класса на распадающийся класс является нераспадающимся классом. В частности, квадрат любого класса, взаимно простого с  $4D$ , является распадающимся классом.

Для доказательства того, что имеется равное число распадающихся и нераспадающихся классов, достаточно доказать, что существует по крайней мере один нераспадающийся класс. Действительно, умножение на нераспадающийся класс задает взаимно однозначное отображение множества классов, взаимно простых с  $4D$ , на себя, которое переставляет распадающиеся и нераспадающиеся классы. Для того чтобы найти нераспадающийся класс, можно поступить следующим образом. Если  $\varepsilon r \neq 1$ , то  $\binom{\varepsilon}{p} \binom{r}{p}$  принимает оба значения  $\pm 1$  и для любого данного  $n$ , взаимно простого с  $4D$ , найдется нечетное  $n'$ , такое, что  $\binom{\varepsilon}{n'} \binom{r}{n'}$  противоположно  $\binom{n}{p_1} \cdots \binom{n}{p_\mu} \binom{n}{p'_1} \cdots \binom{n}{p'_\nu}$ ; согласно китайской теореме об остатках, существует  $n'' \equiv n \pmod{p_1 \cdots p_\mu p'_1 \cdots p'_\nu}$  и  $n'' \equiv n' \pmod{8}$ . Тогда  $\binom{D}{n''} = -1$ , что и требуется. Если  $\varepsilon r = 1$ , то, поскольку  $D \neq 1$ , либо  $\mu$ , либо  $\nu$  должно быть отлично от нуля, и аналогичный метод дает нам  $n''$  с  $\binom{D}{n''} = -1$ .

Остается показать, что  $\binom{D}{-n} = \binom{D}{n}$  при  $D > 0$  и  $\binom{D}{-n} = -\binom{D}{n}$  при  $D < 0$ . Другими словами, остается показать, что  $\binom{D}{-1}$  равно знаку  $D$ . Множители  $\binom{r}{-1}$  и  $\binom{-1}{p_i}$  в  $\binom{D}{-1}$  всегда равны  $+1$ . Множители  $\binom{-1}{p'_i}$  всегда равны  $-1$ , а множитель  $\binom{\varepsilon}{-1}$  равен  $+1$ , если  $\varepsilon = +1$ , и  $-1$ , если  $\varepsilon = -1$ . Следовательно,  $\binom{D}{-1} = \varepsilon (-1)^\nu$ , что также совпадает со знаком  $D$ , что и требовалось доказать.

Это завершает доказательство того, что из квадратичного закона взаимности следуют все теоремы Эйлера. Обратное утверждение (согласно которому из теорем Эйлера следует квадратичный закон взаимности) можно доказать следующим образом<sup>1)</sup>. Дополнительные законы взаимности немедленно следуют из теорем Эйлера при  $D = -1$  и  $D = 2$  (упр. 4). Предположим теперь, что  $D = q$ , где  $q$  — нечетное простое. Квадрат любого класса, взаимно простого с  $4q$ , является распадающимся классом. Легко доказать, что в точности четверть классов, взаимно простых с  $4q$ , являются квадратами (упр. 3). Значит, это правило позволяет найти половину распадающихся классов. Поскольку  $D = q > 0$ , против-

<sup>1)</sup> Это доказательство принадлежит Кронекеру [К1].



положительный распадающемуся классу снова является распадающимся классом. Следовательно, противоположный квадрату будет распадающимся классом. Между квадратами и противоположными квадратам нет пересечений: действительно, из сравнения  $x^2 \equiv z \equiv -y^2 \pmod{4q}$  при  $z$ , взаимно простом с  $4q$ , следовало бы, что  $x$  и  $y$  нечетны, и потому должны выполняться сравнения  $z \equiv 1$  и  $z \equiv -1 \pmod{4}$ . Следовательно, вторая половина распадающихся классов состоит из противоположных квадратам, и мы получаем все распадающиеся классы. Таким образом, нечетное простое  $p \neq q$  распадается тогда и только тогда, когда  $p \equiv \pm x^2 \pmod{4q}$  для некоторого целого  $x$ . То есть если  $p \neq q$  — нечетные простые, то  $q$  является квадратом по модулю  $p$  тогда и только тогда, когда  $p$  или  $-p$  есть квадрат по модулю  $4q$ .

Легко видеть, что это совпадает с квадратичным законом взаимности. Если  $p \equiv 1 \pmod{4}$ , то  $-p$  не может быть квадратом по модулю 4, не говоря о модуле  $4q$ . Доказанная теорема в этом случае утверждает, что  $q$  является квадратом по модулю  $p$  тогда и только тогда, когда  $p$  является квадратом по модулю  $4q$ . Отсюда, конечно, следует, что  $p$  является квадратом по модулю  $q$ . Обратно, если  $p$  — квадрат по модулю  $q$ , скажем  $p \equiv y^2 \pmod{q}$ , то  $p \equiv (y - q)^2 \pmod{q}$ . Поскольку либо  $y$ , либо  $y - q$  нечетно, можно считать, что нечетно  $y$ ,  $y^2 \equiv 1 \equiv p \pmod{4}$ ,  $y^2 \equiv p \pmod{4q}$  (так как  $q$  нечетно), и  $p$  является квадратом по модулю  $4q$ . Таким образом, если  $p \equiv 1 \pmod{4}$ , то  $q$  является квадратом по модулю  $p$  тогда и только тогда, когда  $p$  является квадратом по модулю  $q$ . Аналогично, если  $p \equiv -1 \pmod{4}$ , то  $p$  или  $-p$  является квадратом по модулю  $4q$  только тогда, когда  $-p$  есть квадрат по модулю  $q$ , и если  $p \equiv 3 \pmod{4}$ , то  $q$  является квадратом по модулю  $p$  тогда и только тогда, когда  $-p$  является квадратом по модулю  $q$ . Это и есть квадратичный закон взаимности в формулировке Гаусса.

## Упражнения

1. Предположим, что простые, сравнимые по модулю  $4D$ , в теории дивизоров квадратичных целых детерминанта  $D$  разлагаются одинаковым образом (распадаются, разветвляются или остаются простыми). Докажите, что если  $p_0 \equiv p_1 \pmod{4D}$  и  $p_0 \mid x_0^2 - Dy_0^2$  для взаимно простых  $x_0$  и  $y_0$ , то существуют такие взаимно простые  $x_1$  и  $y_1$ , что  $p_1 \mid x_1^2 - Dy_1^2$ . Это доказывает теорему Эйлера о делителях  $x^2 + ny^2$  при свободном от квадратов  $-n$ . Докажите, что теорема Эйлера тривиальна, если  $-n$  является квадратом. Наконец, выведите случай  $-n = t^2D$  со свободным от квадратов  $D$  из случая  $-n = D$ .

2. Распространите табл. 7.8.1 на все свободные от квадратов детерминанты  $D$  с  $|D| \leq 15$ .

3. Докажите, что в точности четверть классов, взаимно простых с  $4q$  ( $q$  — простое), являются квадратами.

4. Выведите формулы для  $\left(\frac{-1}{p}\right)$ ,  $\left(\frac{2}{p}\right)$ ,  $\left(\frac{-2}{p}\right)$  (дополнительные квадратичные законы взаимности) из теорем Эйлера для  $D = -1, 2$  и  $-2$  соответ-

ственно. [Для  $D = -1$  и  $D = 2$  ни одно простое  $p$  не требует проверки на распадение. При  $D = -2$  необходима одна проверка (если не пользоваться равенством  $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right)$ ).

5. Докажите, что если  $A$  — произвольный дивизор квадратичных целых детерминанта  $D$  и  $a = N(A)$ , то либо  $\left(\frac{D}{a}\right) = +1$ , либо  $\left(\frac{D}{a}\right)$  не определено. Следовательно, образ норменного отображения дивизоров в целые по модулю  $4D$  не содержит половину классов, взаимно простых с  $4D$ , а именно: он не содержит нераспадающихся классов. [В частности, при  $D > 0$  класс  $-1$  является распадающимся.]

6. В основном тексте утверждается: если известно, что в точности половина классов по модулю  $4D$  являются распадающимися и что произведение распадающихся классов снова является распадающимся классом, то отсюда следует, что квадрат любого класса будет распадающимся. Докажите это утверждение, доказывая более общий факт, что произведение двух нераспадающихся классов всегда образует распадающийся класс.

7. Объясните, почему  $\left(\frac{D}{n}\right) = +1$  при  $D = -7$  и  $n = 15$ , хотя  $-7$  не является квадратом по модулю 15.

8. Докажите, что для символов Якоби справедлив квадратичный закон взаимности (если соответствующие символы определены). То есть если  $p$  и  $q$  нечетны и взаимно просты, то

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{при } p \equiv 1 \pmod{4}, \\ \left(\frac{-p}{q}\right) & \text{при } p \equiv -1 \pmod{4}, \end{cases}$$

даже когда  $p$  и  $q$  не являются простыми. Это показывает, что законны вычисления из упр. 4 к § 5.6.

9. Докажите, что если  $D = -n$  является квадратом, то теоремы Эйлера неверны по той простой причине, что  $p \mid x^2 + ny^2$  (при некоторых взаимно простых  $x, y$ ) для всех простых  $p$ . Докажите, что если  $D = t^2 D'$ , то из теорем Эйлера для  $D'$  следуют те же самые теоремы для  $D$ .

## 7.9. Роды классов дивизоров

Задача нахождения группы классов дивизоров данного детерминанта  $D$  приводит к задаче определения, эквивалентны или нет два заданных дивизора. Гаусс заметил, что имеются некоторые простые *необходимые* условия эквивалентности двух дивизоров, и при помощи этих необходимых условий разделил классы дивизоров на множества, которые он назвал *родами*. (Однако Гаусс рассматривал бинарные квадратичные формы, а не дивизоры. См. гл. 8.) Это деление на роды играет важную роль в его втором доказательстве квадратичного закона взаимности.

Два дивизора эквивалентны тогда и только тогда, когда произведение одного из них на сопряженный к другому является главным дивизором. Условия Гаусса, необходимые для эквивалентности дивизоров, получаются из следующих простых условий, необходимых для того, чтобы данный дивизор был главным.

Если  $A$  — дивизор элемента  $x + y \sqrt{D}$ , то  $N(A) = x^2 - Dy^2$ , где  $x$  и  $y$  — целые или, возможно, полуцелые числа. Если  $p$  —

нечетный простой делитель  $D$ , то  $4N(A) = (2x)^2 - D(2y)^2 \equiv \equiv u^2 \pmod{p}$ , где  $u = 2x$  — целое число. Поскольку  $p$  нечетно, возможно деление на 2 по модулю  $p$ , и отсюда следует, что норма главного дивизора должна быть квадратом по модулю  $p$  для любого нечетного простого делителя  $p$  детерминанта  $D$ . Следовательно, если  $A_1$  и  $A_2$  — эквивалентные дивизоры и  $n_1$  и  $n_2$  соответственно — их нормы, то  $A_1 \bar{A}_2$  — главный дивизор и  $n_1 n_2$  должно быть квадратом по модулю  $p$ . Если  $n_1 n_2 \not\equiv 0 \pmod{p}$ , то отсюда легко следует, что  $n_1$  является квадратом по модулю  $p$  тогда и только тогда, когда этим свойством обладает  $n_2$ . (Если  $n_1 n_2 \equiv u^2$ ,  $u \not\equiv 0$  и  $n_1 \equiv v^2$ , то  $v \not\equiv 0$ , возможно деление на  $v$  и  $n_2 \equiv (u/v)^2$  — квадрат по модулю  $p$ . По симметрии, если  $n_1$  не является квадратом по модулю  $p$ , то и  $n_2$  и не является квадратом.) В терминах символа Лежандра это можно выразить в виде равенства  $\left(\frac{n_1}{p}\right) = \left(\frac{n_2}{p}\right)$ . Таким образом, *необходимое условие эквивалентности*  $A_1 \sim A_2$  *состоит в равенстве*  $\left(\frac{n_1}{p}\right) = \left(\frac{n_2}{p}\right)$ , где  $n_1 = N(A_1)$ ,  $n_2 = N(A_2)$  и где предполагается, что  $A_1$  и  $A_2$  взаимно просты с  $p$ .

Если  $D \not\equiv 1 \pmod{4}$ , то есть еще одно необходимое условие эквивалентности, соответствующее простому 2. Если  $D \equiv \equiv 3 \pmod{4}$ , то для любого главного дивизора  $A$  имеем  $N(A) = = x^2 - Dy^2 \equiv x^2 + y^2 \pmod{4}$ , где  $x$  и  $y$  — целые числа. Если  $A$  взаимно прост с 2, то  $N(A)$  нечетна,  $x$  и  $y$  имеют противоположную четность и  $N(A) \equiv 1 \pmod{4}$ . Таким образом, если  $A_1 \sim A_2$  и оба эти дивизора взаимно просты с 2, то  $n_1 n_2 \equiv 1 \pmod{4}$ . Отсюда следует, что  $n_1$  и  $n_2$  одновременно сравнимы по модулю 4 либо с 1 либо с  $-1$ . Если  $D \equiv 2 \pmod{4}$ , то есть другое необходимое условие эквивалентности, но оно сильно отличается от соответствующего условия для  $D \equiv 3 \pmod{4}$ . Если  $D \equiv 2 \pmod{4}$  и  $A$  является главным дивизором, взаимно простым с 2, то  $N(A) = = x^2 - Dy^2$ , где  $x$  и  $y$  — целые и  $x$  нечетно. Таким образом,  $x^2 \equiv 1 \pmod{8}$  и  $-Dy^2 \equiv 0$  или  $-D \pmod{8}$  в зависимости от того, четно или нечетно  $y$ . Если  $D \equiv 2 \pmod{8}$ , то  $N(A) \equiv 1$  или  $-1 \pmod{8}$  и  $N(A) \not\equiv \pm 3 \pmod{8}$ . Следовательно, если  $n_1 \equiv \equiv \pm 1 \pmod{8}$ , то  $n_2 \equiv \pm 1 \pmod{8}$ , и если  $n_1 \equiv \pm 3 \pmod{8}$ , то  $n_2 \equiv \pm 3 \pmod{8}$ , где  $n_1$  и  $n_2$  — нормы эквивалентных дивизоров, взаимно простых с 2. Аналогично, если  $D \equiv -2 \pmod{8}$ , то  $N(A) \equiv 1$  или  $3 \pmod{8}$ , и  $n_1 \equiv 1$  или  $3 \pmod{8}$  тогда и только тогда, когда  $n_2 \equiv 1$  или  $3 \pmod{8}$ , а  $n_1 \equiv 5$  или  $7 \pmod{8}$  тогда и только тогда, когда  $n_2 \equiv 5$  или  $7 \pmod{8}$ . Коротче говоря, если  $D \not\equiv 1 \pmod{4}$  и если мы введем *дополнительный знак*, как указано в табл. 7.9.1, то для дивизоров  $A_1, A_2$ , взаимно простых с 2, *необходимое условие эквивалентности*  $A_1 \sim A_2$  *состоит в том, что*  $n_1$  *и*  $n_2$  *имеют один и тот же дополнительный знак*. Здесь  $n_1 = = N(A_1)$  и  $n_2 = N(A_2)$ . (Заметим, что, согласно дополнительным квадратичным законам взаимности, дополнительный знак равен

Таблица 7.9.1

Дополнительный знак			
$D$	+, если		—, если
$\equiv 3 \pmod{4}$	$n \equiv 1 \pmod{4}$		$n \equiv -1 \pmod{4}$
$\equiv 2 \pmod{8}$	$n \equiv \pm 1 \pmod{8}$		$n \equiv \pm 3 \pmod{8}$
$\equiv -2 \pmod{8}$	$n \equiv 1 \text{ или } 3 \pmod{8}$		$n \equiv 5 \text{ или } 7 \pmod{8}$

$\binom{-1}{n}$ , если  $D \equiv -1 \pmod{4}$ ,  $\binom{2}{n}$ , если  $D \equiv 2 \pmod{8}$ , и  $\binom{-2}{n}$ , если  $D \equiv -2 \pmod{8}$ .)

Пусть  $m$  — количество нечетных простых делителей  $D$ , и пусть  $\varepsilon$  равно 0, если  $D \equiv 1 \pmod{4}$ , и равно 1 в противном случае. Характер дивизора  $A$  определяется как список из  $m + \varepsilon$  знаков  $\pm 1$ , состоящий из  $m$  знаков  $\binom{N(A)}{p_i}$  ( $p_i$  — нечетный простой делитель  $D$ ) вместе с дополнительным знаком, определенным табл. 7.9.1 (с  $n = N(A)$ ) в случае  $\varepsilon = 1$ . Если  $A$  не взаимно прост с  $D$  или, в случае  $\varepsilon = 1$ , не взаимно прост с  $2D$ , то его характер не определен. Для определенности будем записывать эти  $m + \varepsilon$  знаков в порядке  $\binom{N(A)}{p_1}$ ,  $\binom{N(A)}{p_2}$ ,  $\dots$ ,  $\binom{N(A)}{p_m}$ , где  $p_1 < p_2 < \dots < p_m$ , с последующим дополнительным знаком (если он имеется).

Поскольку знаки (если они определены) эквивалентных дивизоров совпадают, мы можем определить *характер класса дивизоров*, при условии что этот класс содержит по крайней мере один дивизор, характер которого определен. Легко доказать (см. § 8.3), что любой дивизор эквивалентен некоторому дивизору, взаимно простому с  $2D$ , и определить таким образом характер класса дивизоров. Однако характер класса дивизоров можно определить, и не доказывая этой теоремы. Для этого достаточно определить *знак в отдельности для каждого простого  $p$* . Для того чтобы определить знак, соответствующий простому  $p$  (включая  $p = 2$  в случае дополнительного знака), достаточно в данном классе найти дивизор  $A$ , взаимно простой с  $p$ . Для этого достаточно найти дивизор, эквивалентный  $(p, *)$ , который взаимно прост с  $p$ . (Заметим, что 2 разветвляется тогда и только тогда, когда  $\varepsilon = 1$ .) За исключением случая  $p = 2$ ,  $D \equiv 3 \pmod{4}$ , такой дивизор равен дивизору элемента  $\sqrt{D}$ , деленному на  $(p, *)$ . В оставшемся случае этот дивизор равен дивизору элемента  $1 - \sqrt{D}$ , деленному на  $(p, *) = (2, *)$ .

В случаях, рассмотренных в § 7.6, классы дивизоров имеют следующие характеры. Если  $D = 67$ , то характер содержит  $1 + 1$  знак. Для класса дивизора  $(-1, *)$  первый знак равен  $-1$  (поскольку  $-1$  не является квадратом по модулю 67), а второй знак также равен  $-1$  (ибо  $-1 \equiv -1 \pmod{4}$ ). Таким образом,

характер этого класса есть — —. Главный класс, конечно, имеет характер + +.

При  $D = -165$  характер состоит из четырех знаков, соответствующих простым 3, 5, 11 и 2. Первые три знака дивизора  $A = (2, *)$  равны  $\left(\frac{2}{3}\right) = -1$ ,  $\left(\frac{2}{5}\right) = -1$ ,  $\left(\frac{2}{11}\right) = -1$ ; четвертый знак находится из замечания, что дивизор элемента  $1 - \sqrt{-165}$  равен  $(2, *) (83, 1)$ , так что  $(2, *) \sim (83, 1)$ , и искомый знак равен  $-1$ , поскольку  $83 \equiv -1 \pmod{4}$ . Таким образом, характер класса дивизора  $A$  есть — — — —. Последние три знака характера дивизора  $B = (3, *)$  равны  $\left(\frac{3}{5}\right) = -1$ ,  $\left(\frac{3}{11}\right) = +1$  и  $-1$  (поскольку  $3 \equiv -1 \pmod{4}$ ); его первый знак находится из соотношения  $(3, *) \sim (5, *) (11, *)$  и равен  $\left(\frac{55}{3}\right) = \left(\frac{1}{3}\right) = +1$ . Следовательно, характер класса  $B$  есть + — + —. Аналогично находится характер класса  $C = (5, *)$ : — — ++. Характеристики остальных классов можно найти простым умножением: для этого достаточно заметить, что *характер произведения двух классов равен произведению их характеристик*. (Характеры умножаются перемножением соответствующих знаков. Для знаков, отвечающих нечетным простым делителям  $p$  детерминанта  $D$ , утверждение о том, что знак произведения равен произведению знаков:  $\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right) \left(\frac{n_2}{p}\right)$ , — было доказано в § 5.6. Для знаков, соответствующих простому 2, его можно проверить при помощи табл. 7.9.1. Это свойство тесно связано со свойством  $\chi(n_1 n_2) = \chi(n_1) \chi(n_2)$  «характеров» из § 6.4. В действительности употребление слова «характер» в теории групп обязано своим происхождением тому, что Гаусс использовал его в соответствующей части «Арифметических исследований».)

Характеры различных классов при  $D = -165$  приведены в табл. 7.9.2. Обратите внимание на то, что различные классы

Таблица 7.9.2.  $D = -165$ ,  $A = (2, *)$ ,  $B = (3, *)$ ,  $C = (5, *)$

Класс дивизора	Имеет характер	Класс дивизора	Имеет характер
$I$	+ + + +	$AB$	— + — +
$A$	— — — —	$AC$	+ + — —
$B$	+ — + —	$BC$	— + + —
$C$	— — + +	$ABC$	+ — — +

дивизоров имеют различные характеры. Это означает, что необходимые условия эквивалентности в данном случае являются *достаточными*: два дивизора с одинаковыми характерами эквивалентны. Уже Эйлер заметил и использовал это удобное свойство детерминанта  $D = -165$  (см. упр. 4).

В следующем случае из § 7.6 ( $D = -163$ ) имеется только главный класс. Характер состоит из одного знака ( $163$  — простое,  $-163 \equiv 1 \pmod{4}$ ) и характер  $I$  есть  $+$ .

При  $D = 79$  характер состоит из двух знаков, и характер  $B = (3, 1)$  равен  $\binom{3}{79} = -\binom{79}{3} = -1$  и  $-1$  (поскольку  $3 \equiv -1 \pmod{4}$ ). Характер  $B^2$  равен  $(- -)^2 = + +$ . Таким образом, классы  $I, B^2, B^4$  имеют характер  $+$   $+$ , а остальные классы  $B, B^3, B^5$  имеют характер  $- -$ . Гаусс назвал множество классов дивизоров с данным характером *родом*. Таким образом, при  $D = 79$  имеется два рода,  $\{I, B^2, B^4\}$  и  $\{B, B^3, B^5\}$ . В предыдущих случаях роды совпадали с классами дивизоров.

В следующем примере из § 7.6 ( $D = -161$ ) характер состоит из 3 знаков ( $D$  имеет два нечетных простых делителя 7 и 23 и  $D \equiv 3 \pmod{4}$ ). Дивизор  $A = (3, 1)$  имеет характер  $- + -$ , а  $B = (7, *)$  — характер <sup>1)</sup>  $+ - -$ . Отсюда можно немедленно найти характеры всех 16 классов  $A^i B^j$ . Они приведены в табл. 7.9.3.

Таблица 7.9.3.  $D = -161, A = (3, 1), B = (7, *)$

Класс дивизора	Характер	Класс дивизора	Характер
$I$	$+$ $+$ $+$	$B$	$+$ $-$ $-$
$A$	$-$ $+$ $-$	$AB$	$-$ $-$ $+$
$A^2$	$+$ $+$ $+$	$A^2B$	$+$ $-$ $-$
$A^3$	$-$ $+$ $-$	$A^3B$	$-$ $-$ $+$
$A^4$	$+$ $+$ $+$	$A^4B$	$+$ $-$ $-$
$A^5$	$-$ $+$ $-$	$A^5B$	$-$ $-$ $+$
$A^6$	$+$ $+$ $+$	$A^6B$	$+$ $-$ $-$
$A^7$	$-$ $+$ $-$	$A^7B$	$-$ $-$ $+$

В этом случае имеется четыре рода  $\{I, A^2, A^4, A^6\}$ ,  $\{A, A^3, A^5, A^7\}$ ,  $\{B, A^2B, A^4B, A^6B\}$ ,  $\{AB, A^3B, A^5B, A^7B\}$ . Гаусс описывал такое деление классов дивизоров на роды, говоря, что  $D = -161$  соответствует классификации IV.4. Под этим он подразумевал, что имеется IV рода, каждый из которых содержит 4 класса. Аналогично,  $D = 79$  соответствует классификации II.3,  $D = -163$  — классификации I.1,  $D = -165$  — классификации VIII.1 и  $D = 67$  — классификации II.1.

В последнем примере из § 7.6 ( $D = 985 = 5 \cdot 197$ ) характер состоит из двух знаков. Характер дивизора  $A = (2, 0)$  равен

<sup>1)</sup> Собственно говоря, первый знак характера дивизора  $B$  не определен. Характер его *класса* имеет первый знак  $+$ , поскольку  $(7, *) \sim (23, *)$  и  $\binom{23}{7} = +1$ .



$\binom{2}{5} \binom{2}{197} = \binom{2}{5} \binom{2}{5} = -$  — . Таким образом,  $D = 985$  соответствует классификации II.3 с родами  $\{I, A^2, A^4\}$  и  $\{A, A^3, A^5\}$ .

С замечанием Эйлера о том, что в точности половина классов по модулю  $4D$  являются распадающимися классами, тесно связано замечание Гаусса, согласно которому в действительности встречается *ровно половина возможных характеров*. (См. табл. 7.9.4.)

### Таблица 7.9.4

$D$	Число возможных характеров	Число встречающихся характеров
67	4	2 (+ +, - -)
- 165	16	8 (характеры, произведение +) которых равно
- 163	2	1 (+)
79	4	2 (+ +, - -)
- 161	8	4 (+ + +, - + -, + - -, - - +)
985	4	2 (+ +, - -)

Из квадратичного закона взаимности (или, что, по существу, то же самое, из теорем Эйлера) легко получить, что фактически может встретиться *не более* половины возможных характеров (упр. 1). Метод второго доказательства Гаусса квадратичного закона взаимности заключается в том, чтобы доказать обратное: если известно, что фактически встречается не более половины возможных характеров, то отсюда следует закон квадратичной взаимности (см. § 7.11). Поэтому для доказательства квадратичного закона взаимности достаточно доказать, что в действительности встречается не более половины возможных характеров. Гаусс смог доказать это, подсчитывая *двусторонние классы* (см. § 7.10) и сравнивая их с числом встречающихся характеров.

Заметим, что число возможных характеров равно  $2^{m+\varepsilon}$  и что число родов равно числу действительно встречающихся характеров. Следовательно, теорема Гаусса о числе характеров эквивалентна утверждению, что существуют  $2^{m+\varepsilon-1}$  родов. Классификацию IV.4, II.3, I.1, VIII.1, II.1 и т. д. детерминантов  $D$  можно рассматривать как *разложение числа классов*  $h = g \cdot n$ , где  $g =$  IV, II, I, VIII, II и т. д. — число родов, а  $n = 4, 3, 1, 1, 1$  и т. д. — число классов в роде. (Утверждение, что все роды содержат одинаковое число классов, немедленно следует из того, что характер произведения равен произведению характеров.) Теорема Гаусса утверждает, что первый сомножитель в этом разложении найти относительно легко:  $g = 2^{m+\varepsilon-1}$ , где  $m$  — число нечетных простых делителей  $D$ , а  $\varepsilon = 1$ , если  $D \equiv 2$  или  $3 \pmod{4}$ , и  $\varepsilon = 0$  в противном случае. Однако связь между детерминантом  $D$  и самим

числом классов  $h$  является очень тонкой, и тот факт, что первый сомножитель  $g$  просто связан с  $D$ , означает лишь, что для второго сомножителя это не так.

## Упражнения

1. Используя квадратичный закон взаимности, покажите, что в действительности встречается не более половины всех возможных характеров. Точнее, покажите, что во всяком действительно встречающемся характере число минусов четно. [Воспользуйтесь символом Якоби.] Применяя теорему Дирихле о простых в арифметической прогрессии, докажите, что в действительности встречается *ровно* половина всех возможных характеров.

2. Докажите, что если  $k = x^2 + ny^2$ , где  $n > 0$ , то для того, чтобы  $k$  было простым числом, необходимо выполнение следующих условий: (1)  $x$  взаимно просто с  $ny$ , (2)  $x$  и  $ny$  имеют противоположную четность (за исключением тривиального случая  $x^2 + ny^2 = 2$ ) и (3) единственными представлениями  $k = u^2 + nv^2$  являются представления, в которых  $u = \pm x$ ,  $v = \pm y$ , или, если  $n = 1$ , то  $u = \pm y$ ,  $v = \pm x$ .

3. Докажите, что при  $n = 165$  необходимые условия из упражнения 2 являются и достаточными. [Если  $k$  не простое, то дивизор числа  $x + y\sqrt{-165}$  либо имеет вид  $A_1A_2$ , где  $A_1$  и  $A_2$  взаимно просты, либо является степенью простого дивизора  $(p, u)^n$ , где  $n > 1$ . В первом случае  $\overline{A_1A_2}$  является главным дивизором, отличным как от  $A_1A_2$ , так и от  $\overline{A_1A_2}$ , что противоречит (3). Во втором случае существует главный дивизор с нормой  $k$ , который делится на  $p$ , что также противоречит (3).]

4. Докажите, что если  $a$  и  $b$  — такие положительные целые, что  $ab$  свободно от квадратов,  $ab \not\equiv 3 \pmod{4}$ , и каждый род детерминанта  $D = -ab$  содержит только один класс, то следующие условия необходимы и достаточны для того, чтобы  $k = ax^2 + by^2$  было простым числом: (1)  $ax$  и  $by$  взаимно просты; (2)  $ax$  и  $by$  имеют противоположную четность; (3) единственными представлениями  $k = au^2 + bv^2$  являются такие представления с  $u = \pm x$ ,  $v = \pm y$ . [Не ограничивая общности, можно предположить, что  $a = p_1p_2 \dots p_n$  нечетно. Тогда  $ak$  — норма главного дивизора вида  $(p_1, *) (p_2, *) \dots (p_n, *) A$ .] Имеющие такой вид числа  $n = ab$  (такие, как  $+165$ ) Эйлер называл *удобными числами* (numerus idoneus). При полном исследовании удобных чисел необходимо рассмотреть случаи  $ab \equiv 3 \pmod{4}$  и/или  $ab$  не свободно от квадратов. См. упр. 8—12 к § 8.1.

5. Найдите все значения  $x$ , меньшие 50, для которых  $165 + x^2$  является простым числом. [Кроме очевидных исключений, соответствующих условиям (1) и (2), есть еще 5 исключений, отвечающих условию (3), что в итоге дает 7 простых.]

6. Докажите, что 5 — удобное число. Докажите, что  $1301 = 36^2 + 5$  — простое число. [Начиная с 1301, вычитайте последовательно 5, 15, 25, 35, 45, ... . Обратите внимание на то, что эта прогрессия содержит только один квадрат.]

7. Гипотеза Ферма о числах вида  $x^2 + 5y^2$  (см. § 1.7) состоит в том, что если  $p_1$  и  $p_2$  — простые, которые сравнимы с 3 по модулю 4 и которые в десятичной записи оканчиваются на 3 или 7, то  $p_1p_2 = x^2 + 5y^2$ . Докажите, что эта гипотеза верна. [Из сравнений  $p \equiv 3$  или  $7 \pmod{20}$  следует, что  $p$  распадается и его простые дивизоры принадлежат одному неглавному классу, совпадающему с родом.]

8. Докажите, что нечетное простое  $p$  имеет вид  $p = x^2 - Dy^2$  только тогда, когда  $p$  или  $p + D$  есть квадрат по модулю  $4D$ . Эйлер считал, что это условие является также и достаточным. Действительно, наименьшие значения  $D$ , при которых это не выполняется, довольно велики. Одно из них нашел Лагранж [L2, разд. 84]. Примером Лагранжа является случай  $D = 79$ ,  $p = 101$ ; тогда  $p + D$  — квадрат по модулю  $4D$ , но  $p \neq x^2 - Dy^2$ . Более

того, Лагранж заметил, что нельзя ответить на вопрос о том, справедливо ли равенство  $p = x^2 - Dy^2$ , не зная ничего, кроме класса  $p$  по модулю  $4D$ . Действительно,  $101 \equiv 733 \pmod{4D}$ ,  $733$  — простое и  $733 = x^2 - Dy^2$  (при  $D = 79$ ). Переформулируйте эти утверждения в терминах классов и родов простых делителей чисел  $101$  и  $733$  и докажите их. Меньшее значение  $D$ , противоречащее гипотезе Эйлера, приведено в упр. 9 к § 8.4.

## 7.10. Двусторонние классы

Гаусс называл класс дивизоров (хотя, конечно, в его формулировке речь шла о классах бинарных квадратичных форм, а не дивизоров) *двусторонним* классом, если этот класс совпадает со своим сопряженным. Это определение можно сформулировать иначе, если сказать, что любой дивизор  $A$  из данного класса удовлетворяет соотношению  $A \sim \bar{A}$ , или, проще говоря, что квадрат этого класса равен главному классу. Гаусс обнаружил, что число двусторонних классов (или по крайней мере верхнюю границу для него) можно найти непосредственно, не прибегая к квадратичному закону взаимности или к теоремам Эйлера, и что это дает достаточно информации о возможных характерах классов дивизоров, чтобы *отсюда можно было вывести* квадратичный закон взаимности (и, следовательно, все теоремы Эйлера из § 7.8). Этот параграф посвящен подсчету числа двусторонних классов. Вывод квадратичного закона взаимности приведен в следующем параграфе.

Если  $p$  — разветвленное простое, то  $(p, *)^2 \sim I$  и класс дивизора  $(p, *)$  является двусторонним. Кроме того, при  $D > 0$  в двустороннем классе лежит  $(-1, *)$ . Следовательно, любое произведение  $(p_1, *) (p_2, *) \dots (p_k, *)$ , где  $p_1, p_2, \dots, p_k$  — разветвленные простые или, при  $D > 0$ ,  $p_1$  может быть равно  $-1$ , лежит в двустороннем классе. Прямое изучение примеров из § 7.6 позволяет убедиться, что таким образом получают все двусторонние классы, т. е. любой двусторонний класс содержит дивизор вида  $(p_1, *) (p_2, *) \dots (p_k, *)$ . [При  $D = 67$  оба класса являются двусторонними; один содержит  $I$  — пустое произведение,  $(-1, *) \times (2, *)$ ,  $(-1, *) (67, *)$  и  $(2, *) (67, *)$ , второй содержит  $(-1, *)$ ,  $(2, *)$ ,  $(67, *)$  и  $(-1, *) (2, *) (67, *)$ . При  $D = -165$  дивизоры  $A = (2, *)$ ,  $B = (3, *)$ ,  $C = (5, *)$  и их произведения лежат во всех 8 возможных классах. Если  $D = -163$ , то единственный класс является двусторонним и содержит как пустое произведение  $I$ , так и  $(163, *)$ . При  $D = 79$  двусторонними являются классы  $I$  и  $B^3$ , где  $B = (3, 1)$ . Первый из них содержит  $I$ ,  $(2, *)$ ,  $(-1, *) \times (79, *)$  и  $(-1, *) (2, *) (79, *)$ , а второй  $(-1, *)$ ,  $(79, *)$ ,  $(-1, *) (2, *)$  и  $(2, *) (79, *)$ . Если  $D = -161$ , то двусторонними являются классы  $I$ ,  $A^4$ ,  $B$ ,  $A^4 B$ , где  $A = (3, 1)$ ,  $B = (7, *)$ . Они содержат  $I$  и  $(7, *) (23, *)$ ;  $(2, *)$  и  $(2, *) (7, *) (23, *)$ ;  $(7, *)$  и  $(23, *)$ ;  $(2, *) (7, *)$  и  $(2, *) (23, *)$  соответственно. При

$D = 985$  имеется два двусторонних класса — классы  $I$  и  $A^3$ , где  $A = (2, 0)$ ; первый из них содержит  $I, (-1, *), (-1, *) (5, *) \times \times (197, *)$  и  $(5, *) (197, *)$ , а второй  $(5, *), (-1, *) (5, *), (-1, *) (197, *)$  и  $(197, *)$ .]

В этом параграфе мы найдем число двусторонних классов в два этапа. На первом этапе мы докажем, что замеченное выше явление закономерно, т. е. каждый двусторонний класс содержит дивизор вида  $(p_1, *) (p_2, *) \dots (p_k, *)$ , где  $p_i$  — разветвленные простые или, при  $D > 0$ ,  $p_1$  может быть равно  $-1$ . На втором этапе мы сосчитаем число различных классов, которые содержат дивизоры такого вида.

Рассмотрим сначала случай  $D < 0$  и  $D \equiv 2$  или  $3 \pmod{4}$ . Каждый дивизор можно привести циклическим методом к дивизору  $A_0$ , который не приводится этим методом:

$$\begin{array}{cccc} r_0 & r_1 & r_0 & \dots \\ a_0 & a_1 & a_0 & \dots \end{array}$$

где  $a_1 \geq a_0$  и условие делимости  $x + y \sqrt{D}$  на  $A_0$  выражено сравнением  $x + yr_0 \equiv 0 \pmod{a_0}$ . Если  $A \sim A_0$  и  $A$  — двусторонний дивизор, т. е.  $A \sim \bar{A}$ , то  $A_0 \sim A \sim \bar{A} \sim \bar{A}_0$ . Если  $a_1 > a_0$ , то, применяя циклический метод к  $\bar{A}_0$ , мы увеличим его норму. Поэтому из теоремы § 7.7 следует, что эквивалентность  $A_0 \sim \bar{A}_0$  влечет за собой равенство  $A_0 = \bar{A}_0$ . Тогда  $A_0$  делит как  $r_0 - \sqrt{D}$ , так и  $r_0 + \sqrt{D}$ . Следовательно,  $A_0$  делит  $2r_0$ , а тем самым и  $a_0$  делит  $2r_0$ . Но  $a_0$  делит  $r_0^2 - D$ , а потому и  $(2r_0)^2 - 4D$ , таким образом,  $a_0$  делит  $4D$ . Поскольку все простые числовые делители  $4D$  являются разветвленными простыми ( $D \equiv 2$  или  $3 \pmod{4}$ ), мы получаем отсюда, что  $A_0$  имеет требуемый вид  $(p_1, *) (p_2, *) \dots (p_k, *)$ . Если  $a_0 = a_1$ , то надо воспользоваться другим методом<sup>1)</sup>. Предположим, что дивизор  $B$  определен условием:  $A_0 \bar{B}$  является дивизором числа  $r_0 + a_0 - \sqrt{D}$ . Пусть  $N(B) = b$ . Тогда  $a_0 b = r_0^2 - D + 2a_0 r_0 + a_0^2 = a_0 a_1 + 2a_0 r_0 + a_0^2$ ,  $b = 2(a_0 + r_0)$ . Поскольку  $b$  делит  $(r_0 + a_0)^2 - D$ ,  $b$  должно также делить  $4(r_0 + a_0)^2 - 4D = b^2 - 4D$  и  $b \mid 4D$ . Следовательно,  $B \sim A_0$  — дивизор требуемого вида.

Рассмотрим теперь случай  $D < 0$ ,  $D \equiv 1 \pmod{4}$ . Этот случай отличается от предыдущего только тем, что  $r_0$  и  $r_1$  являются полуцелыми и  $a_0 a_1 = [(2r_0)^2 - D]/4$ . Поскольку  $a_0$  делит  $2r_0$  (что справедливо при  $a_1 \neq a_0$ ), мы получаем, что  $a_0 \mid D$  (а не только  $a_0 \mid 4D$ ), и  $A_0$  должен иметь нужный вид. При  $a_1 = a_0$  определим  $B$  условием:  $A_0 \bar{B}$  является дивизором числа  $r_0 + a_0 - \frac{1}{2} \sqrt{D}$ . Тогда, как и требуется,  $N(B)$  делит  $D$ .

<sup>1)</sup> Например, при  $D = -165$  циклический метод не приводит  $(13, 2) \sim \sim (13, -2)$ , и  $(13, 2) \sim (2, *) (3, *) (5, *) \sim (13, -2) \sim (2, *) (11, *)$ .

Теперь рассмотрим случай  $D > 0$ ,  $D \equiv 2$  или  $3 \pmod{4}$ . Каждый дивизор  $A$  эквивалентен некоторому дивизору  $A_0$ , обладающему тем свойством, что применение к нему циклического метода возвращает нас к  $A_0$ . Если  $A \sim \bar{A}$ , то  $A_0 \sim \bar{A}_0$ . Поэтому достаточно показать, что если  $A_0 \sim \bar{A}_0$ , то  $A_0$  эквивалентен дивизору требуемого вида  $(p_1, *) (p_2, *) \dots (p_k, *)$ . Основной факт, который для этого нужен, состоит в том, что *цикл для  $\bar{A}_0$  совпадает с записанным в обратном порядке циклом для  $A_0$* . То есть если, применяя циклический метод к  $A_0$ , мы получаем

$$\begin{array}{ccccccc} r_0 & r_1 & \dots & r_{m-1} & r_0 & r_1 & \dots \\ a_0 & a_1 & \dots & a_{m-1} & a_0 & a_1 & \dots \end{array}$$

то применение его к  $\bar{A}_0$  дает

$$\begin{array}{ccccccc} r_{m-1} & r_{m-2} & \dots & r_1 & r_0 & r_{m-1} & \dots \\ a_0 & a_{m-1} & \dots & a_2 & a_1 & a_0 & \dots \end{array}$$

Ясно, что  $\bar{A}_0$  делит  $r_{m-1} - \sqrt{D}$  и что  $N(r_{m-1} - \sqrt{D}) < 0$ . Для того чтобы доказать, что применение циклического метода к  $\bar{A}_0$  дает  $\bar{A}_{m-1}$ , необходимо и достаточно доказать, что  $N(r_{m-1} + |a_0| - \sqrt{D}) > 0$ , т. е. что  $(r_{m-1} + |a_0|)^2 > D$ . При доказательстве неравенства  $r_j > 0$  в § 7.5 мы показали, что  $(r_{j+1} + |a_{j+1}|)^2 < D$  при  $a_j > 0$  и  $(r_{j+1} - |a_{j+1}|)^2 < D$  при  $a_j < 0$ . Другими словами,  $(r_{j+1} - |a_{j+1}|)^2 < D$  при всех  $j$ . При  $j + 1 = m - 1$  это дает  $r_{m-1}^2 - 2r_{m-1}|a_{m-1}| + a_{m-1}^2 < D$ ,  $a_0 a_{m-1} - 2r_{m-1}|a_{m-1}| + a_{m-1}^2 < 0$ ,  $-|a_0| - 2r_{m-1} + |a_{m-1}| < 0$ ,  $a_0^2 + 2r_{m-1}|a_0| + a_0 a_{m-1} > 0$ ,  $(|a_0| + r_{m-1})^2 > D$ , что и требуется. Тогда по той же причине применение циклического метода к  $\bar{A}_{m-1}$  дает  $\bar{A}_{m-2}$ , и т. д.

Если  $A_0 \sim \bar{A}_0$ , то, согласно теореме из § 7.7,  $\bar{A}_0$  должен входить в период  $A_0$ , скажем  $\bar{A}_0 = A_j$ . Тогда  $A_0 = \bar{A}_j$  и, как только что было показано,  $A_1 = \bar{A}_{j-1}$ ,  $A_2 = \bar{A}_{j-2}$ , и т. д. Поскольку  $N(A_j)$  меняет знак и  $N(A_0) = N(\bar{A}_0) = N(A_j)$ , индекс  $j$  должен быть четным, скажем  $j = 2k$ . Тогда  $A_k = \bar{A}_{j-k} = \bar{A}_k$ . Таким образом,  $A_k$  делит как  $r_k - \sqrt{D}$ , так и  $r_k + \sqrt{D}$ , и  $a_k$  делит  $2r_k$ . Как и раньше, отсюда следует, что  $a_k$  делит  $4D$  и что  $A_k$  имеет требуемый вид.

Изменения, которые необходимы в оставшемся случае  $D > 0$ ,  $D \equiv 1 \pmod{4}$ , очень просты, и мы оставляем их читателю.

Коротко говоря, мы показали, что дивизор является двусторонним тогда и только тогда, когда он эквивалентен дивизору, делящему  $4D$  (если  $D \equiv 2$  или  $3 \pmod{4}$ ) или  $D$  (если  $D \equiv 1 \pmod{4}$ ).

Поэтому для того чтобы сосчитать все неэквивалентные двусторонние дивизоры, достаточно сосчитать все неэквивалентные дивизоры, делящие  $4D$  или  $D$ .

Число разветвленных простых равно  $m + \varepsilon$ , так как при  $D \equiv 1 \pmod{4}$  разветвленными простыми являются нечетные простые делители  $D$ , а при  $D \equiv 2$  или  $3 \pmod{4}$  к ним добавляется 2. Поэтому при  $D < 0$  имеется  $2^{m+\varepsilon}$  дивизоров вида  $(p_1, *) (p_2, *) \dots (p_k, *)$  (включая пустое произведение  $I$ ). Каждый из них эквивалентен по крайней мере одному другому, а именно своему дополнению в дивизоре  $\sqrt{D}$  или, если  $(2, *)$  делит его, но не делит  $\sqrt{D}$ , своему дополнению в дивизоре  $2\sqrt{D}$ . Таким образом, при  $D < 0$  имеется самое большее  $2^{m+\varepsilon-1}$  двусторонних классов. То же самое справедливо при  $D > 0$ , но доказательство несколько менее элементарно. При  $D > 0$  имеется  $2^{m+\varepsilon+1}$  дивизоров вида  $(p_1, *) (p_2, *) \dots (p_k, *)$ , поскольку в этом случае допускается дивизор  $(-1, *)$ . Теперь мы должны доказать, что каждый из них эквивалентен по крайней мере трем другим. Для этого достаточно доказать, что  $I$  эквивалентен по крайней мере трем другим дивизорам. Применяя циклический метод к  $I$ , мы снова получаем  $I$  (применение этого метода к любому главному дивизору дает  $I$ ), и, поскольку знак нормы чередуется, первое возвращение должно произойти на четном шаге, скажем  $A_0 = I$ ,  $A_{2k} = I$ ,  $A_j \neq I$  при  $0 < j < 2k$ . Тогда, как было показано выше,  $A_k$  имеет вид  $(p_1, *) (p_2, *) \dots (p_k, *)$ . Кроме того, абсолютная величина нормы  $A_k$  меньше, чем  $|a_{k-1}a_k| = |r_k^2 - D| = D - r_k^2 < D$ . Поэтому  $A_k$  отличен от дивизора  $\sqrt{D}$  и отличен от своего дополнения в дивизоре  $\sqrt{D}$  (или, если  $(2, *)$  делит  $A_k$ , но не делит  $\sqrt{D}$ , отличен от своего дополнения в дивизоре  $2\sqrt{D}$ ). Таким образом  $I$ ,  $A_k$ , дивизор  $\sqrt{D}$  и дополнение к  $A_k$  дают 4 различных главных дивизора требуемого вида. Следовательно, в любом случае существует не более  $2^{m+\varepsilon-1}$  двусторонних классов.

Поскольку  $2^{m+\varepsilon}$  равно числу всех возможных характеров, только что доказанную теорему можно переформулировать как утверждение о том, что число двусторонних классов не превосходит половины числа возможных характеров.

## Упражнения

Если  $D < 0$ , то имеются  $2^{m+\varepsilon}$  дивизоров вида  $(p_1, *) (p_2, *) \dots (p_k, *)$ , а если  $D > 0$ , то их число равно  $2^{m+\varepsilon+1}$ . В каждом из следующих случаев определите, какой из данных дивизоров является главным, и, опираясь на это, найдите число двусторонних классов.

- |                |                |
|----------------|----------------|
| 1. $D = -30$ . | 4. $D = 210$ . |
| 2. $D = -31$ . | 5. $D = 61$ .  |
| 3. $D = 31$ .  | 6. $D = 59$ .  |



7. Докажите, что если  $D > 0$  — простое, отличное от 2, то основная единица имеет норму  $-1$  тогда и только тогда, когда  $D \equiv 1 \pmod{4}$ , и норму  $+1$  тогда и только тогда, когда  $D \equiv 3 \pmod{4}$ .

8. Докажите, что если  $D = pq$ , где  $p$  и  $q$  — простые, сравнимые с 3 по модулю 4, то либо  $(p, *)$ , либо  $(q, *)$  (но не оба одновременно) является главным дивизором.

9. Докажите, что если  $D$  — (положительное) простое, сравнимое с 1 по модулю 4, то цикл  $I$ , скажем  $I \sim A_1 \sim A_2 \sim \dots$ , содержит следующие друг за другом дивизоры с  $N(A_i) = -N(A_{i+1})$ . Заключите отсюда, что это решает задачу Ферма о нахождении представления  $D = u^2 + v^2$ . Примените этот метод к случаям  $D = 13$  и  $D = 233$  («Disquisitiones Arithmeticae», Art. 265).

## 7.11. Второе доказательство Гаусса квадратичного закона взаимности

Гаусс [G3] утверждал, что он открыл квадратичный закон взаимности совершенно самостоятельно в то время, когда он еще ничего не знал о работах своих предшественников. Хотя и трудно этому поверить, нет никаких сомнений в том, что доказательство Гаусса этого закона в его «Арифметических исследованиях»<sup>1)</sup> было первым правильным доказательством. Фактически Гаусс привел там два совершенно различных доказательства этого закона: одно в четвертом разделе и другое — в пятом. Смит [S3] охарактеризовал доказательство из четвертого раздела (о котором впоследствии Гаусс [G3] говорил, что оно было первым найденным им доказательством) как «отталкивающее всех изучающих его, кроме самых усердных из них» — по крайней мере в той форме, в которой Гаусс изложил это доказательство. (При этом Смит рекомендует это доказательство в редакции Дирихле как изложенное «с той замечательной ясностью, которой отмечены его [Дирихле] математические работы».) Доказательство из пятого раздела, по существу, совпадает с приведенным ниже.

Гаусс изложил это доказательство на языке теории бинарных квадратичных форм, и он рассматривал квадратичный закон взаимности как теорему о решении квадратичных сравнений. Если доказательство Гаусса рассматривать с этой точки зрения, то оно кажется очень далеким от самой теоремы и по этой причине — весьма неудовлетворительным. Если же перевести это доказательство на язык теории дивизоров квадратичных целых и принять точку зрения § 7.8, согласно которой в теореме говорится о распадении простых в арифметике квадратичных целых, то связь между теоремой и ее доказательством оказывается совершенно естественной. Поэтому неудивительно, что именно второе доказательство Гаусса в 1859 г. привело Куммера к доказательству высших законов взаимности для регулярных простых показателей.

В конце § 7.9 было замечено, что число классов можно разложить в виде  $h = g \cdot n$ , где  $g, n$  — «классификация», которой соот-

<sup>1)</sup> Следует помнить, что Гаусс опубликовал их в 24 года.

ветствует  $D$ , т. е.  $g$  — число родов, а  $n$  — число классов в роде. В то же время число классов можно представить в виде  $h = sa$ , где  $s$  — число различных классов, которые являются квадратами других классов, а  $a$  — число двусторонних классов. (В терминах теории групп это немедленно следует из того, что возведение в квадрат является гомоморфизмом, ядро которого состоит из  $a$  элементов, а образ — из  $s$  элементов.) Для того чтобы в этом убедиться, предположим, что  $A_1, A_2, \dots, A_a$  — список дивизоров, выбранных по одному из каждого из  $a$  двусторонних классов. Два класса имеют один и тот же квадрат тогда и только тогда, когда  $B^2 \sim C^2$ , где  $B$  — дивизор из одного класса, а  $C$  — дивизор из другого класса. Последнее выполняется тогда и только тогда, когда  $(B\bar{C})^2 \sim I$ , что справедливо в том и только в том случае, когда  $C \sim A_i B$  для некоторого  $i = 1, 2, \dots, a$ . Таким образом, в точности  $a$  классов имеют такой же квадрат, как и класс произвольного данного  $B$ , поэтому число различных квадратов равно  $s = h/a$  и  $h = sa$ , что и требовалось доказать.

Ясно, что  $s \leq n$ , так как квадрат любого класса принадлежит главному роду. Следовательно,  $g \leq a$ , и оценка  $a$  из предыдущего параграфа показывает, что число  $g$  действительно встречающихся характеров не превосходит половины числа возможных характеров. Из этой теоремы Гаусс вывел квадратичный закон взаимности и все дополнительные законы. Шаги следующего доказательства и их номера взяты из разд. 262 «Арифметических исследований», хотя терминология полностью изменена.

I. Если  $p$  (простое) сравнимо с  $-1$  по модулю 4, то  $\left(\frac{-1}{p}\right) = -1$ . Рассмотрим квадратичные целые с  $D = -1$ . В этом случае характер состоит из одного знака, а именно, характера по модулю 4. Если  $p \equiv -1 \pmod{4}$  и  $\left(\frac{-1}{p}\right) = +1$ , то  $p$  должно было бы распадаться и его простые множители имели бы характер  $-1$ . Поскольку главный класс имеет характер  $+1$ , тогда встретились бы оба возможных характера, что противоречит доказанной выше теореме. Следовательно,  $p \equiv -1 \pmod{4}$  влечет за собой  $\left(\frac{-1}{p}\right) \neq +1$ , что и требовалось доказать.

II. Если  $p \equiv 1 \pmod{4}$ , то  $\left(\frac{-1}{p}\right) = +1$ . Рассмотрим  $D = p$ . Характер состоит из одного знака, а именно, квадратичного характера по модулю  $p$ . Согласно теореме, характер  $-1$  не может встретиться, поэтому  $(-1, *)$  должен иметь характер  $+1$ , что и требовалось доказать.

III. Если  $p \equiv 1 \pmod{8}$ , то  $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = +1$ . Рассмотрим  $D = p$ . Тогда характер состоит из одного знака. Следовательно,  $\left(\frac{q}{p}\right) = +1$  для любого распадающегося простого  $q$ , и, поскольку  $\left(\frac{-1}{p}\right) = +1$  согласно II, мы получаем, что и  $\left(\frac{-q}{p}\right) = +1$ . Но 2 рас-

падает, так как норма числа  $(1 - \sqrt{D})/2$  делится на 2, а само оно на 2 не делится.

IV. Если  $p \equiv 3$  или  $5 \pmod{8}$ , то  $\left(\frac{2}{p}\right) = -1$ . Рассмотрим  $D = 2$ . Тогда характер состоит из одного знака, а именно, знака  $+1$  для дивизоров с нормой  $\equiv \pm 1 \pmod{8}$  и знака  $-1$  для дивизоров с нормой  $\equiv \pm 3 \pmod{8}$ . Характер  $-1$  не может встретиться, поэтому  $p$ , сравнимое с  $\pm 3$  по модулю 8, не может быть нормой дивизора квадратичных целых детерминанта  $D = 2$ . Следовательно,  $\left(\frac{2}{p}\right) = -1$ .

V. Если  $p \equiv 5$  или  $7 \pmod{8}$ , то  $\left(\frac{-2}{p}\right) = -1$ . Доказательство совпадает с доказательством IV, если  $D = 2$  заменить на  $D = -2$ .

VI. Если  $p \equiv 3 \pmod{8}$ , то  $\left(\frac{-2}{p}\right) = +1$ . Действительно,  $\left(\frac{-2}{p}\right) = \left(\frac{+2}{p}\right) \left(\frac{-1}{p}\right) = (-1)^2 = +1$ .

VII. Если  $p \equiv 7 \pmod{8}$ , то  $\left(\frac{2}{p}\right) = +1$ . В самом деле,  $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) \left(\frac{-1}{p}\right) = (-1)^2 = 1$ .

VIII. Если  $p \equiv 1 \pmod{4}$  и  $q$  — простое, для которого  $\left(\frac{q}{p}\right) = -1$ , то  $\left(\frac{p}{q}\right) = -1$ . Рассмотрим  $D = p$ . Характер состоит из единственного знака, который должен быть равен  $+1$ . Следовательно, если  $\left(\frac{q}{p}\right) = -1$ , то  $q$  не может распадаться, что и требовалось доказать.

IX. Если  $p \equiv -1 \pmod{4}$  и  $\left(\frac{q}{p}\right) = -1$ , то  $\left(\frac{-p}{q}\right) = -1$ . Рассмотрим  $D = -p$ . Характер состоит из одного знака, а именно, из квадратичного характера по модулю  $p$ , и  $q$  может распадаться только тогда, когда этот характер равен  $+1$ .

X. Если  $p \equiv 1 \pmod{4}$  и  $\left(\frac{q}{p}\right) = +1$ , то  $\left(\frac{p}{q}\right) = +1$ . Если  $q \equiv 1 \pmod{4}$ , то, согласно VIII, из  $\left(\frac{p}{q}\right) = -1$  следовало бы, что  $\left(\frac{q}{p}\right) = -1$ . Если  $q \equiv -1 \pmod{4}$ , то, согласно II,  $\left(\frac{-q}{p}\right) = \left(\frac{q}{p}\right) \times \left(\frac{-1}{p}\right) = 1$ , и из IX следует, что  $\left(\frac{p}{q}\right) \neq -1$ .

XI. Если  $p \equiv -1 \pmod{4}$  и  $\left(\frac{q}{p}\right) = +1$ , то  $\left(\frac{-p}{q}\right) = +1$ . Если  $q \equiv 1 \pmod{4}$ , то, согласно II и VIII,  $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right) \left(\frac{p}{q}\right) = +1$ . В оставшемся случае  $q \equiv -1 \pmod{4}$  положим  $D = pq$ . Тогда характер состоит из двух знаков, а именно, квадратичного характера по модулю  $p$  и квадратичного характера по модулю  $q$ . Согласно I, характер  $(-1, *)$  равен  $-1, -1$ . Следовательно, встречаются только характеры  $++$  и  $--$ . Поскольку  $(-1, *) \times (p, *) (q, *)$  является дивизором  $\sqrt{D}$ ,  $(q, *) \sim (-1, *) (p, *)$ . Характер класса дивизоров  $(q, *)$  и  $(-1, *) (p, *)$  равен  $\left(\frac{q}{p}\right)$ ,  $\left(\frac{-p}{q}\right)$ . Это завершает доказательство.

Итак, из I и II следует, что  $\left(\frac{-1}{p}\right) \equiv p \pmod{4}$ , из III—VIII следует, что  $\left(\frac{2}{p}\right)$  равно  $+1$ , если  $p \equiv \pm 1 \pmod{8}$ , и  $-1$ , если  $p \equiv \pm 3 \pmod{8}$ , а из VIII—XI следует, что  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$  при  $p \equiv 1 \pmod{4}$ ,  $\left(\frac{-p}{q}\right) = \left(\frac{q}{p}\right)$  при  $p \equiv -1 \pmod{4}$ . Следовательно, квадратичные законы взаимности и теоремы Эйлера из § 7.8 доказаны.

### Упражнения

1. Докажите, что число классов в роде равно 1 тогда и только тогда, когда каждый дивизор эквивалентен дивизору вида  $(p_1, *) (p_2, *) \dots (p_k, *)$ .

2. В добавление к приведенным выше доказательствам VI и VII Гаусс предложил следующие варианты доказательства. В VI положим  $D = 2p$ . Тогда имеются 4 характера, из которых могут встретиться не более двух. Можно вычислить характер  $(-1, *)$  и точно узнать, какие именно два характера входят. Требуемое заключение получится, если рассмотреть характер класса  $(p, *) \sim (-1, *) (2, *)$ . В VII положим  $D = -p$  и заметим, что 2 распадается. Восполните детали этих доказательств.

3. Покажите, что утверждение, согласно которому в действительности встречается точно половина всех возможных характеров, равносильно утверждению, что каждый класс в главном роде является квадратом. Гаусс доказал оба эти утверждения («Disquisitiones», Art. 286), используя теорию тернарных квадратичных форм для построения дивизора с данным квадратом в главном роде. Ср. с упр. 1 к § 7.9.

## ГАУССОВА ТЕОРИЯ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ

### 8.1. Другие группы классов дивизоров

В предыдущей главе *группы классов дивизоров* были определены для свободных от квадратов детерминантов  $D$ . Основная цель данной главы состоит в том, чтобы показать связь между этими группами и *группами классов бинарных квадратичных форм*, которые ввел Гаусс в «Арифметических исследованиях». Для того чтобы установить эту связь в простейшем виде, необходимо сначала обобщить понятие группы классов дивизоров таким образом, чтобы оно включало все возникающие в теории Гаусса случаи. Требуемое обобщение можно полностью мотивировать на основе теории дивизоров для более общих видов «квадратичных целых», вообще не используя в обсуждении бинарные квадратичные формы. Это является предметом настоящего параграфа. В следующих параграфах мы покажем, каким образом эта теория связана с теорией бинарных квадратичных форм.

С наивной точки зрения «квадратичные целые детерминанта  $D$ » представляют собой просто множество всех чисел вида  $x + y \sqrt{D}$ , где  $x$  и  $y$  — целые. В следующем эвристическом обсуждении именно такие числа мы будем считать квадратичными целыми вида  $x + y \sqrt{D}$ . При  $D \equiv 1 \pmod{4}$  ( $D$  свободно от квадратов) в предыдущей главе было дано другое определение квадратичных целых (мы допускали знаменатели, равные числу 2); для того чтобы избежать путаницы, мы исключим случай  $D \equiv 1 \pmod{4}$  из следующего эвристического обсуждения. Естественно также исключить случай, когда  $D$  является квадратом, поскольку тогда квадратичное целое  $x + y \sqrt{D}$  совпадает с обыкновенным целым. Наша цель состоит в том, чтобы развить теорию дивизоров квадратичных целых  $x + y \sqrt{D}$ . Так как для случая свободного от квадратов  $D$  эта цель уже была достигнута в предыдущей главе, то следует рассмотреть случай, когда  $D = t^2 D'$ , где  $D'$  — свободное от квадратов целое, а  $t$  — положительное целое, большее 1. Тогда квадратичные целые  $x + y \sqrt{D} = x + yt \sqrt{D'}$  содержатся среди квадратичных целых детерминанта  $D'$ , определенных в предыдущей главе. Введенное в гл. 7 понятие дивизора квадратичного целого детерминанта  $D'$  естественным образом приводит к определению дивизора квадратичного целого вида  $x + y \sqrt{D}$ . Однако такое

определение еще не дает удовлетворительной теории дивизоров, поскольку в рассматриваемом случае по следующей причине *не выполняется основная теорема*.

Предположим, что  $x + y\sqrt{D}$  и  $u + v\sqrt{D}$  в теории дивизоров квадратичных целых детерминанта  $D'$  имеют дивизоры  $A$  и  $B$  соответственно. Тогда утверждение о том, что  $x + y\sqrt{D}$  делит  $u + v\sqrt{D}$  в арифметике квадратичных целых детерминанта  $D$ , конечно, должно означать существование таких целых  $m$  и  $n$ , что  $u + v\sqrt{D} = (x + y\sqrt{D})(m + n\sqrt{D})$ . Если последнее равенство выполняется, то  $B = AC$ , где  $C$  — дивизор числа  $m + n\sqrt{D}$ , и делимость  $B$  на  $A$  является *необходимым* условием делимости  $u + v\sqrt{D}$  на  $x + y\sqrt{D}$ . Основная теорема утверждает, что это условие является также и достаточным. Однако, как показывают примеры, в данном случае это утверждение не обязательно выполняется. Например, если  $D = -9$ ,  $D' = -1$ ,  $t = 3$ ,  $x + y\sqrt{D} = 3 + 0\sqrt{-9}$ ,  $u + v\sqrt{D} = 3 + \sqrt{-9}$ , то  $u + v\sqrt{D} = 3 + 3\sqrt{-1} = (x + y\sqrt{D})(1 + \sqrt{-1})$ , т. е.  $x + y\sqrt{D}$  делит  $u + v\sqrt{D}$ , если рассматривать эти числа как квадратичные целые детерминанта  $D'$ . Таким образом, выполняется необходимое условие  $A \mid B$ . Однако  $x + y\sqrt{D}$  не делит  $u + v\sqrt{D}$ , если эти числа рассматривать как квадратичные целые детерминанта  $D$ . Действительно, частное  $1 + \sqrt{-1}$  не имеет вида  $m + n\sqrt{D}$ . Следовательно, условие  $A \mid B$  не является достаточным.

Прежде всего следует заметить, что нарушения справедливости основной теоремы всегда имеют простой характер — такой же, как и в приведенном выше примере, когда при делении исчезают нужные делители числа  $t$ . Однако в целом теория дивизоров квадратичных целых детерминанта  $D$  остается верной, даже если число  $D$  не является свободным от квадратов. Для того чтобы стало ясно, в каком смысле следует понимать последнее утверждение, рассмотрим сначала случай, когда  $D' \not\equiv 1 \pmod{4}$ . В этом случае квадратичными целыми детерминанта  $D'$  являются  $\{x + y\sqrt{D'} : x, y \text{ — целые}\}$ , и такое квадратичное целое будет квадратичным целым детерминанта  $D$  тогда и только тогда, когда  $t$  делит  $y$ . Таким образом, допуская некоторую вольность речи, можно сказать, что среди каждых  $t$  квадратичных целых детерминанта  $D'$  одно является квадратичным целым детерминанта  $D$ . Целое  $t$  называется *индексом* <sup>1)</sup> квадратичных целых детерминанта  $D$  в квадратичных целых детерминанта  $D'$ . Предположим, что  $x + y\sqrt{D}$  и  $u + v\sqrt{D}$  имеют дивизоры  $A$  и  $B$  соответственно и что  $A$  делит  $B$ . Тогда, согласно основной теореме,  $u + v\sqrt{D} = (x + y\sqrt{D})(m +$

<sup>1)</sup> В терминах теории групп это есть не что иное, как индекс подгруппы.



$+ n\sqrt{\bar{D}'}$ ), и возникает вопрос, делится ли  $n$  на  $t$ . Если  $x + y\sqrt{\bar{D}}$  взаимно просто с  $t$ , то  $t$  должно делить  $n$ . Мы можем доказать это утверждение следующим образом.

Если данное равенство умножить на  $x - y\sqrt{\bar{D}}$  (освободиться от иррациональности в знаменателе), то мы получим  $(u + v\sqrt{\bar{D}}) \times \times (x - y\sqrt{\bar{D}}) = (x^2 - Dy^2)(m + n\sqrt{\bar{D}'})$ . Если  $x + y\sqrt{\bar{D}}$  взаимно просто с  $t$ , то этим же свойством обладают  $x - y\sqrt{\bar{D}}$  и  $x^2 - Dy^2$ . Через  $k$  обозначим целое  $x^2 - Dy^2$ . Если  $x + y\sqrt{\bar{D}}$  взаимно просто с  $t$ , то целые  $t$  и  $k$  взаимно просты и существуют такие целые  $a$  и  $b$ , что  $ak + bt = 1$ . Тогда число  $m + n\sqrt{\bar{D}'} = (ak + bt)(m + n\sqrt{\bar{D}'}) = a[k(m + n\sqrt{\bar{D}'})] + bt(m + n\sqrt{\bar{D}'} = a[(u + v\sqrt{\bar{D}}) \times \times (x - y\sqrt{\bar{D}})] + (btm + bn\sqrt{\bar{D}})$  имеет вид  $c + d\sqrt{\bar{D}}$ , что и требовалось доказать.

Условие « $x + y\sqrt{\bar{D}}$  взаимно просто с  $t$ » является очень естественным. Если оно не выполнено, то существует простой дивизор  $P$ , который делит как  $t$ , так и  $x + y\sqrt{\bar{D}}$ . Но тогда  $x \equiv x + yt\sqrt{\bar{D}'} = x + y\sqrt{\bar{D}} \equiv 0 \pmod{P}$ , и отсюда следует, что  $x$  делится на простое целое  $p$ , делящееся на  $P$ . Тогда  $x + y\sqrt{\bar{D}} = p(x' + yt'\sqrt{\bar{D}'})$ , где  $x' = x/p$  и  $t' = t/p$ . Это означает, что при делении на  $x + y\sqrt{\bar{D}}$  естественно разделить сначала на целое  $p$ , а затем на квадратичное целое  $x' + yt'\sqrt{\bar{D}'}$ , рассматриваемое как квадратичное целое для меньшего детерминанта  $D'' = (t')^2 D' < < D$ .

Короче говоря, в теории дивизоров квадратичных целых детерминанта  $D$  (которую они наследуют как квадратичные целые детерминанта  $D'$ ) основная теорема будет выполняться, если исключить деление на элементы  $x + y\sqrt{\bar{D}}$ , не взаимно простые с  $t$ . Это исключение является естественным, поскольку элемент  $x + y\sqrt{\bar{D}}$ , не взаимно простой с  $t$ , делится на некоторое целое, и задачу можно свести к соответствующей задаче с меньшим детерминантом  $D$ .

Дальше мы можем очевидным образом определить понятие *главных* и *эквивалентных* дивизоров для квадратичных целых  $x + y\sqrt{\bar{D}}$  (временно сохраняя предположение, что  $D$  и  $D' \not\equiv \equiv 1 \pmod{4}$ ). Дивизор квадратичных целых детерминанта  $D'$  называется *главным для квадратичных целых детерминанта  $D$* , если он является дивизором некоторого элемента  $x + y\sqrt{\bar{D}}$ . Два дивизора  $A$  и  $B$  для квадратичных целых детерминанта  $D'$  называются *эквивалентными для квадратичных целых детерминанта  $D$* , если условие « $AC$  — главный дивизор» равносильно условию « $BC$  — главный дивизор». Другими словами,  $A$  эквивалентен  $B$ , если при замене в произвольном дивизоре (для квадратичных целых детерминанта  $D'$ ), делящемся на  $A$ , дивизора  $A$  на  $B$

новый дивизор будет главным дивизором квадратичных целых детерминанта  $D$  тогда и только тогда, когда главным был исходный дивизор.

Как и в предыдущих случаях, из этих определений немедленно следует, что эквивалентность является рефлексивным, симметричным и транзитивным отношением, согласованным с умножением дивизоров. Таким образом, можно перемножать *классы* дивизоров, и класс  $I$  является единицей относительно этого умножения. Однако классы дивизоров не обязательно образуют *группу*, поскольку могут найтись дивизоры  $A$ , для которых не существует такого дивизора  $B$ , что  $AB \sim I$ , т. е. могут существовать дивизоры  $A$ , для которых нет обратного элемента относительно умножения. Однако, как и в случае нарушения основной теоремы, дивизор  $A$  может не иметь мультипликативного обратного только тогда, когда он не взаимно прост с  $t$ . Это можно доказать следующим образом.

Если  $A$  взаимно прост с  $t$ , то  $A\bar{A}$  является дивизором некоторого целого — обозначим его  $k$ , — взаимно простого с  $t$ . Наше утверждение состоит в том, что  $A\bar{A} \sim I$ . Ясно, что если  $I \cdot C$  — главный дивизор, то дивизор  $A\bar{A} \cdot C$  также является главным: он совпадает с дивизором элемента  $k(x + y\sqrt{D})$ , где  $x + y\sqrt{D}$  — квадратичное целое с дивизором  $C$ . Мы должны доказать, что если  $A\bar{A} \cdot C$  — главный дивизор, то  $I \cdot C$  также является главным дивизором. Это утверждение немедленно следует из основной теоремы. Действительно, если квадратичное целое  $u + v\sqrt{D}$  имеет дивизор  $A\bar{A}C$ , то, разделив его на взаимно простое с  $t$  число  $k$ , дивизор которого равен  $A\bar{A}$ , мы получим квадратичное целое  $x + y\sqrt{D}$  с дивизором  $C$ . Следовательно,  $A\bar{A} \sim I$  и дивизор  $A$  имеет обратный к нему элемент относительно умножения, что и требовалось доказать.

Таким образом, если ограничиться рассмотрением дивизоров, взаимно простых с  $t$ , то соответствующие классы дивизоров будут составлять *группу*. Эта группа называется *группой классов дивизоров* детерминанта  $D$ . Как и в случае детерминантов, свободных от квадратов, эта группа конечна, и при данном  $D$  может быть найдена явно при помощи циклического метода. Мы докажем эти утверждения позже в данной главе.

Остается определить группу классов дивизоров при  $D' \equiv 1 \pmod{4}$ . (Если  $D \equiv 1 \pmod{4}$ , то  $t$  нечетно,  $t^2 \equiv 1 \pmod{4}$  и  $D' \equiv 1 \pmod{4}$ , так что этот случай включается в случай  $D' \equiv 1 \pmod{4}$ .) В этом случае квадратичное целое детерминанта  $D'$  можно записать в виде  $u + v\omega$ , где  $u$  и  $v$  — целые и  $\omega = (1 - \sqrt{D'})/2$ . Такое квадратичное целое имеет вид  $x + y\sqrt{D}$  тогда и только тогда, когда  $v$  делится на  $2t$ . То же самое рассуждение,

что и выше, показывает теперь, что *основная теорема справедлива* для квадратичных целых вида  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$  в случае деления на элементы, взаимно простые с  $2t$ . Если очевидным образом определить понятие *главного* дивизора и *эквивалентности* дивизоров, то, в точности так же как и выше, можно перемножать *классы эквивалентности* дивизоров; эта операция имеет единицу, и классы дивизоров, взаимно простые с индексом  $2t$ , образуют *группу*, которая называется *группой классов дивизоров* для квадратичных целых  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$ .

Общий случай группы классов дивизоров можно описать следующим образом. *Порядком*<sup>1)</sup> квадратичных целых детерминанта  $D'$  называется подмножество вида  $\{x + y\sqrt{D'} : x, y \text{ — целые, } y \text{ делится на } s\}$  при  $D' \not\equiv 1 \pmod{4}$  или вида  $\{x + y\omega : x, y \text{ — целые, } y \text{ делится на } s\}$  при  $D' \equiv 1 \pmod{4}$ ,  $\omega = (1 - \sqrt{D'})/2$ . Положительное целое  $s$  называется *индексом* данного порядка в полном порядке всех квадратичных целых детерминанта  $D'$ . Глава 7 была посвящена группам классов дивизоров в случае  $s = 1$ . Для каждого свободного от квадратов  $D'$  и для каждого положительного  $s$  существует и притом единственный порядок квадратичных целых детерминанта  $D'$ , который имеет индекс  $s$ . При  $D' \not\equiv 1 \pmod{4}$  этот порядок состоит из элементов, которые мы называли выше квадратичными целыми детерминанта  $s^2D'$ . Если  $D' \equiv 1 \pmod{4}$  и  $s$  четно, скажем  $s = 2t$ , то он состоит из  $\{x + y\sqrt{t^2D'} : x, y \text{ — целые}\}$ . При  $D' \equiv 1 \pmod{4}$  и нечетном  $s$  этот порядок образует множество  $\{x + y\sqrt{s^2D'} : x, y \text{ — целые или } x, y \text{ — полуцелые}\}$ . Рассмотренные выше случаи приводят к следующим определениям.

Предположим, что задан порядок квадратичных целых детерминанта  $D'$ . Дивизор  $A$  для квадратичных целых детерминанта  $D'$  назовем *главным* относительно данного порядка, если он является дивизором некоторого элемента из этого порядка. Дивизоры  $A$  и  $B$  будем называть *эквивалентными* относительно данного порядка, если дивизор  $AC$  является главным относительно этого порядка в том и только в том случае, когда  $BC$  является главным относительно этого же порядка. Тогда корректно определено умножение классов эквивалентности (т. е. класс эквивалентности дивизора  $AB$  зависит только от классов  $A$  и  $B$ ), и класс  $I$  является

<sup>1)</sup> Эту терминологию ввел Дедекин ( [D7], § 171). Она перекликается с гауссовыми «порядками» бинарных квадратичных форм, но не связана с ними непосредственно. В определении порядков Дедекин не использовал их явного описания — такого, как в данном параграфе. Он дал аксиоматическое определение порядков, применимое к другим типам алгебраических «целых». (Подобное определение порядков см. в упр. 5.) В действительности Дедекин говорил, что «... эта новая теория идеалов... при  $n=2$  совпадает с теорией различных *порядков* бинарных квадратичных форм...» (Bull. des Sciences Math. Ser. 2, v. 1 (1877), pp. 217—218).

мультипликативной единицей. Пусть  $s$  — индекс данного порядка. Тогда множество всех классов эквивалентности дивизоров, взаимно простых с  $s$ , образует *группу*, которая называется группой классов дивизоров. Точнее, если дивизор  $A$  взаимно прост с  $s$ , то дивизор  $A\bar{A}$  эквивалентен  $I$ . Это можно доказать следующим образом.

Дивизор  $A\bar{A}$  является дивизором некоторого целого числа  $a$ , поэтому очевидно, что если  $I \cdot C$  — главный дивизор, то и  $A\bar{A} \cdot C$  является главным дивизором. Обратно, если  $A\bar{A}C$  — главный дивизор, то он является дивизором некоторого элемента  $x + y\sqrt{D}$  из данного порядка. Так как дивизор числа  $a$  делит дивизор элемента  $x + y\sqrt{D}$ , то  $x + y\sqrt{D} = a(u + v\sqrt{D'})$ , где  $u + v\sqrt{D'}$  — квадратичное целое (не обязательно принадлежащее данному порядку) с дивизором  $C$ . Для того чтобы доказать, что  $I \cdot C$  является главным дивизором, достаточно доказать, что  $u + v\sqrt{D'}$  принадлежит рассматриваемому порядку. Далее, в силу предположения о том, что дивизор  $A$  взаимно прост с  $s$ , целое число  $a$  взаимно просто с  $s$ . Следовательно, существуют такие целые  $k$  и  $m$ , что  $ak + ms = 1$ . Тогда элемент  $u + v\sqrt{D'} = (ak + ms)(u + v\sqrt{D'}) = k(x + y\sqrt{D}) + ms(u + v\sqrt{D'})$  принадлежит данному порядку, так как непосредственно из определения следует, что для любого квадратичного целого  $u + v\sqrt{D'}$  целое  $s(u + v\sqrt{D'})$  принадлежит порядку индекса  $s$ .

В упр. 1 и 6 речь идет о вычислении групп классов дивизоров в двух частных случаях. Дальнейшие примеры будут приведены в § 8.5 — после того, как мы разовьем эффективные методы *классификации* дивизоров относительно порядка, т. е. методы определения, эквивалентны или нет два данных дивизора относительно данного порядка.

## Упражнения

1. Докажите следующие утверждения о группе классов дивизоров порядка  $\{x + y\sqrt{-11} : x, y \text{ — целые}\}$ . (a)  $(3, 1)$  не является главным дивизором. (b) Если  $(2)$  — дивизор числа 2 (который является простым дивизором при  $D' = -11$ ), то  $(2)$  и  $(3, 1)$  — главные дивизоры, хотя дивизор  $(3, 1)$  не является главным. (c) Дивизор  $(3, 1)^2$  не является главным, но  $(3, 1)^3$  — главный дивизор. Следовательно,  $(3, 1)^2 \sim (3, -1)$ . (d)  $(5, 2) \sim (3, 1)$ . (e)  $(11, *) \sim I$ . (f) 7, 13, 17, 19 остаются простыми. (g)  $(23, 9) \sim (3, 1)$ . (h) 29 остается простым. (i) 31 распадается на два простых дивизора, один из которых эквивалентен  $(3, 1)$ , а другой  $(3, 1)^2$ . Эти вычисления наводят на мысль, что  $I$ ,  $(3, 1)$  и  $(3, 1)^2$  образуют систему представителей для группы классов дивизоров. Для доказательства этого утверждения требуется только доказать, что каждый дивизор эквивалентен некоторому дивизору с меньшей нормой, если норма исходного дивизора еще недостаточно мала. (j) Каждый дивизор является главным для группы классов дивизоров порядка  $\{x + y\sqrt{-11} : x, y \text{ — целые или полуцелые}\}$ . (k) Если дивизор  $(p, u)$  не является главным в рассматриваемой группе классов дивизоров, то эквивалентности  $(p, u) \sim (3, 1)$  или  $(p, u) \sim (3, 1)^2$  могут быть получены умноже-

нием элемента с дивизором  $(p, u)$  на  $2(1 \pm \sqrt{-11})$  с последующим делением на 4.

2. Используя упр. 1, приведите пример трех дивизоров  $A, B, C$ , таких, что  $AC \sim I, BC \sim I, A \not\sim B$ . Выведите отсюда, что класс дивизора  $C$  не имеет мультипликативного обратного.

3. Для классификации дивизоров в более общих группах классов дивизоров, определенных в этом параграфе, нельзя пользоваться циклическим методом, если не внести в него некоторых изменений. Для того чтобы убедиться в этом, примените циклический метод к дивизору  $(13, 5)$  в случае  $D' = -1, t = 6, D = -36$ . В результате получится период из двух дивизоров, ни один из которых не эквивалентен  $(13, 5)$ . Теория, изложенная в трех следующих параграфах, в основном посвящена преодолению этой трудности, с той целью чтобы можно было пользоваться циклическим методом для классификации дивизоров как в новых, так и в старых случаях.

4. Докажите, что если дивизор  $A$  взаимно прост с индексом  $s$  данного порядка, то  $A$  является главным дивизором тогда и только тогда, когда  $A \sim I$ .

5. Покажите, что подмножество квадратичных целых детерминанта  $D'$  является порядком тогда и только тогда, когда оно обладает следующими двумя свойствами: (1) суммы и разности элементов этого подмножества снова принадлежат данному подмножеству и (2) это подмножество содержит обыкновенные целые в качестве собственного подмножества (т. е. каждое обыкновенное целое  $x + 0 \cdot \sqrt{D'}$  принадлежит этому подмножеству, и по крайней мере один элемент данного подмножества не является обыкновенным целым). [Рассмотрите наименьшее положительное целое или полуцелое, которое может встретиться как коэффициент при  $\sqrt{D'}$  в элементе данного подмножества.]

6. Найдите группу классов дивизоров, соответствующую порядку  $\{x + y\sqrt{18} : x, y \text{ — целые}\}$ . [Методы гл. 7 позволяют для данного дивизора легко найти все квадратичные целые, имеющие этот дивизор. В нашем случае формула для таких целых имеет вид  $\pm (x + y\sqrt{2})\epsilon^n$ , где  $\epsilon = (1 - \sqrt{2})^2$ . Для того чтобы определить, принадлежит ли некоторый элемент данному порядку, достаточно вычислить его по модулю 3; получающееся выражение периодически по  $n$ . Докажите, что  $(-1, *) \sim (2, *) \not\sim I$ . Покажите, что каждый дивизор эквивалентен или  $I$ , или  $(-1, *)$ .]

7. Если детерминант  $D$  отрицателен,  $D \equiv -3 \pmod{8}$ , но  $D \neq -3$ , то группа классов дивизоров порядка  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$  содержит некоторый элемент порядка 3 (т. е. элемент, который сам не принадлежит главному классу, но его куб принадлежит). Это впервые заметил Гаусс (Disquisitiones Arithmeticae, Art. 256, VI). Ср. с упр. 1. [Куб дивизора целого  $(1 - \sqrt{D})/2$  является главным относительно рассматриваемого порядка. При  $D \neq -3$  сам дивизор числа  $(1 - \sqrt{D})/2$  не является главным.]

8. Положительное число  $n$  называется *удобным*, если квадрат любого класса из группы классов дивизоров порядка  $\{x + y\sqrt{-n} : x, y \text{ — целые}\}$  является главным классом. Докажите, что число, удобное в смысле упр. 4 из § 7.9, является удобным и в этом новом смысле. [См. упр. 1 к § 7.11.] Предположим, что  $n$  — удобное число. Пусть  $ab = n, k = ax^2 + by^2$ , где  $ax$  и  $by$  — взаимно простые числа противоположной четности. Допустим, что  $k$  представимо в виде  $au^2 + bv^2$  только тогда, когда  $u = \pm x, v = \pm y$ . Докажите, что в этом случае число  $k$  простое. [Не ограничивая общности, можно предположить, что  $a$  нечетно. Тогда дивизор целого  $ax + y\sqrt{-n}$  имеет вид  $AK$ , где  $A = (p_1, *) (p_2, *) \dots (p_n, *)$  и дивизор  $K$  взаимно прост с индексом  $s$ . Если  $K = K_1 K_2$ , то  $AK_1 \bar{K}_2$  — главный дивизор, и это дает существенно другое представление числа  $k$  в виде  $k = au^2 + bv^2$ .] Эйлер привел список из 65 удобных чисел, наибольшее из которых равно 1848. С тех пор не было



найденно больше ни одного удобного числа, и была выдвинута гипотеза, что список Эйлера исчерпывает все такие числа. Удобные числа называются также *подходящими* (idoneal). Список Эйлера приведен в [E10, E12]. См. также [S4].

9. Эйлер применил свой метод удобных чисел для нахождения больших простых чисел. Наибольшее найденное им при помощи этого метода простое равно  $18\,518\,809 = 197^2 + 1848 \cdot 100^2$ . Количество труда, которое требуется для доказательства того, что это число является простым, представляет собой интересную меру сложности (даже для столь быстрого и искусного в вычислениях математика, как Эйлер) задачи нахождения простых чисел такой величины. Докажите, что это число является простым. [Метод Эйлера изложен в [E12]. Кроме него можно использовать следующий метод Гаусса (метод «исключающих»). Пусть  $A = 197^2 + 1848 \cdot 100^2$ . Надо доказать, что единственными решениями уравнения  $x^2 + 1848y^2 = A$  являются  $x = \pm 197$ ,  $y = \pm 100$ . (Поскольку 1848 — удобное число, а числа 197 и  $100 \cdot 1848$  взаимно просты и имеют противоположную четность, отсюда следует, что  $A$  — простое.) По модулю 1848 данное уравнение превращается в  $x^2 \equiv 1$ . Поскольку  $1848 = 8 \cdot 3 \cdot 7 \cdot 11$ , это сравнение эквивалентно сравнениям  $x^2 \equiv 1 \pmod{8}$ ,  $x^2 \equiv 1 \pmod{3}$ ,  $x^2 \equiv 1 \pmod{7}$  и  $x^2 \equiv 1 \pmod{11}$ . То есть  $x \equiv 1 \pmod{2}$  и  $x \equiv \pm 1 \pmod{3, 7, 11}$ . Согласно китайской теореме об остатках, отсюда следует, что  $x$  принимает одно из значений  $\pm 1, \pm 43, \pm 155, \pm 197$  по модулю  $2 \cdot 3 \cdot 7 \cdot 11 = 462$ . Поскольку можно считать, что  $x$  положительно и  $x < \sqrt{A}$ , это исключает все числа, кроме чисел из 8 последовательностей  $1 + 462k$  ( $0 \leq k \leq 9$ ),  $-1 + 462k$  ( $1 \leq k \leq 9$ ),  $43 + 462k$  ( $0 \leq k \leq 9$ ),  $-43 + 462k$  ( $1 \leq k \leq 9$ ),  $\dots$ ,  $-197 + 462k$  ( $1 \leq k \leq 9$ ). Всего имеется 76 таких чисел: 75 чисел в добавление к известному решению  $x = 197$ . Метод исключаящих следующим образом устраняет большую часть этих возможностей. Пусть 5 — «исключающее». Для первой из 8 последовательностей рассматриваемое уравнение по модулю 5 превращается в  $(1 + 462k)^2 + 1848y^2 = A$ ,  $(1 + 2k)^2 \equiv 4 - 3y^2 \pmod{5}$ . Поскольку  $y^2 \equiv 0, \pm 1$ , отсюда следует, что  $(1 + 2k)^2 \equiv 4, 1$  или  $2 \pmod{5}$ . Тогда  $(1 + 2k)^2 \equiv 1$  или  $4$  и  $1 + 2k \equiv 1, 2, 3$  или  $4 \pmod{5}$ , так как  $z^2 \not\equiv 2$ . Это исключает  $k = 2$  и  $k = 7$ . Аналогично, если в качестве исключаящего взять 13 (13 — следующее за 5 простое, которое не делит 1848), то мы находим, что  $(1 + 7k)^2 \equiv -3 - 2y^2 \pmod{13}$ , где  $y^2 \equiv 0, \pm 1, \pm 3, \pm 4$ . Тогда  $(1 + 7k)^2 \equiv -3, -5, -1, -9 \equiv 4, 3, -11 \equiv 2$  или  $5$ . Таким образом,  $(1 + 7k)^2 \equiv -3, -1, 4$  или  $3$  и  $1 + 7k \equiv \pm 6, \pm 5, \pm 2$  или  $\pm 4 \pmod{13}$ . Это исключает  $k = 0, 4, 5$  и  $9$ . Исключающие 3, 7, 11 тоже можно использовать, несмотря на то что они делят 1848. Например, в случае исключаящего 3 уравнение  $x^2 + 3 \cdot 616y^2 = A$  дает  $x^2 + 3y^2 \equiv 4 \pmod{9}$ . (Напомним, что число можно привести по модулю 9, если сложить все его цифры.) Так как  $y^2 \equiv 0$  или  $1 \pmod{3}$ , то  $3y^2 \equiv 0$  или  $3 \pmod{9}$  и  $x^2 \equiv 4$  или  $1 \pmod{9}$ . Если  $x = 1 + 462k \equiv 1 + 3k \pmod{9}$ , то отсюда следует, что  $2 \cdot 3k \equiv 3$  или  $0 \pmod{9}$ ,  $2k \equiv 0$  или  $1 \pmod{3}$ . Таким образом,  $k \not\equiv 1 \pmod{3}$ . Аналогично, находим  $x^2 \equiv -6, 8, 22$  или  $1 \pmod{49}$ ,  $x \equiv 1 + 7 \cdot 3k \pmod{49}$ ,  $6k \equiv -1, 1, 3, 0 \pmod{7}$ ,  $k \not\equiv 2, 3, 5 \pmod{7}$ . После этого остаются лишь возможности  $k = 6$  или  $8$ . Их можно исключить, рассматривая сравнения по модулю 11. Действительно,  $x^2 \equiv 1, -10, 23, -32, -43$  или  $-54 \pmod{121}$ , что при  $x = 1 + 462k$  дает  $-4k \equiv 0, -1, 2, -3, -4, -5 \pmod{11}$ . Рассмотрим теперь последовательность  $-1 + 462k$ . Используя сравнения  $x^2 \equiv 1$  или  $4 \pmod{9}$  (см. выше), мы получаем, что  $k \not\equiv 2 \pmod{3}$ . Сравнение  $x^2 \equiv 1$  или  $4 \pmod{5}$  дает  $k \not\equiv 3 \pmod{5}$ . Так как  $x^2 \equiv 1, -6, 8$  или  $22 \pmod{49}$ , то  $-6k \equiv -1, 1, 3, 0 \pmod{7}$  и  $k \not\equiv 2, 4, 5 \pmod{7}$ . Аналогично, для исключаящего 11 простой модификацией предыдущего случая мы получаем, что  $4k \equiv 0, -1, 2, -3, -4, -5 \pmod{11}$ . Из оставшихся чисел (1, 6, 7) эти сравнения исключают только 1. Используя исключаящее 13, получим  $-1 + 7k \equiv \pm 2, \pm 4, \pm 5, \pm 6 \pmod{13}$ . Аналогично, 17 дает  $-1 + 3k \equiv 0, \pm 1, \pm 3, \pm 6, \pm 7$ . Но это не исключает ни 6, ни 7. Однако исключаящее



19 исключает и 6, и 7. Простые изменения этих вычислений исключают также все элементы последовательности  $43 + 462k$ , однако в последовательности  $-43 + 462k$  число  $k = 3$  «выживает» как при всех этих исключениях, так и при исключении при помощи 23. Это происходит потому, что  $(-43 + 462 \cdot 3)^2 + 1848y^2 = A$  дает  $y^2 = 9045$ . Неравенство  $95^2 = 9025 < 9045 < 96^2$  показывает, что равенство  $y^2 = 9045$  невозможно. Однако, как ясно из приведенных выше исключений, сравнение  $y^2 \equiv 9045$  разрешимо по модулю 3, 5, 7, 11, 13, 17, 19, 23. При исключениях по этим модулям остается еще одно из этих 75 чисел, а именно:  $x = -155 + 462 \cdot 6$ . Это число может быть решением, только если 6315 — квадрат. Однако  $80^2 = 6400 > 6315 > 79^2$ , и 6315 не является квадратом. Случай  $x = 197 + 462 \cdot 6$  проходит через все эти исключения, кроме исключения по модулю 23. Однако проверка по модулю 23 является *единственной*, которая исключает данное число. По-видимому, эффективнее исключить его прямым методом — не используя исключаящее 23.]

10. Эйлер без доказательства сформулировал [E12] следующий критерий проверки, является ли данное число  $n$  удобным: положительное целое  $n$  является удобным тогда и только тогда, когда все числа из множества  $\{x^2 + n: x$  взаимно просто с  $n$  и  $x^2 + n < 4n\}$  либо являются простыми, либо удвоенными простыми, либо квадратами простых, либо степенями числа 2. Покажите, что критерий Эйлера правильно классифицирует 11 и 13. Считая критерий Эйлера справедливым, найдите все удобные числа между 80 и 89.

11. Докажите, что критерий Эйлера является необходимым условием, т. е. если  $n$  — удобное число, то оно удовлетворяет критерию Эйлера. [Пусть  $AK$  — дивизор элемента  $x + \sqrt{-n}$ , где  $A$  равен произведению простых дивизоров числа 2, а  $K$  взаимно прост с 2. Если  $K = I$ , то  $x^2 + n$  равно степени числа 2. В противном случае  $K$  делится на  $(p, u)$ , где  $p$  взаимно просто с индексом порядка  $\{x + y\sqrt{-n}: x, y \text{ — целые}\}$ . Пусть  $K_1$  — дивизор, полученный из  $K$  заменой  $(p, u)$  на  $(p, -u)$ . Тогда  $AK_1$  — дивизор  $a + b\sqrt{-n}$ , где  $a^2 + nb^2 = x^2 + n$ . Таким образом,  $b^2 = 0$  или 1. Рассмотрим сначала случай  $b^2 = 0$ . Тогда  $A$  и  $K_1$  являются дивизорами целых чисел. Отсюда следует, что  $K = (p, u)^2$ , и мы должны доказать, что  $A = I$ .  $A$  равен дивизору числа  $2^k$  при некотором  $k$ . Если  $k > 0$ , то 4 делит  $x^2 + n$  и  $n \equiv 3 \pmod{4}$ . Случай  $n \equiv 3 \pmod{8}$  можно рассмотреть, используя упр. 7. Если  $n \equiv 7 \pmod{8}$ , то  $k > 1$  и 4 делит  $x + \sqrt{-n}$ , что невозможно. Наконец, рассмотрим случай  $b^2 = 1$ . Тогда  $AK_1$  должен быть сопряжен с  $AK$ . Отсюда следует, что  $A = \bar{A}$  и  $K = (p, u)$ . Если 2 распадается или остается простым, то  $A$  является дивизором числа  $2^k$  при некотором  $k \geq 0$ . Как и раньше, можно исключить случай  $k > 0$ . Если 2 разветвляется, то  $A = (2, *)^k$  для некоторого  $k \geq 0$ . При этом  $k < 2$ , поскольку 2 не делит  $x + y\sqrt{-n}$ . Следовательно,  $x^2 + n$  равно  $p$  или  $2p$ , что и требовалось показать.]

12. Докажите достаточность критерия Эйлера. [Эта задача, оказывается, не решена. Диксон [D2, т. 1, с. 363] сообщает, что этот критерий был доказан Ф. Грубе в 1874 г. Однако обращение к работе Грубе [G9] показывает, что Грубе явно признает, что ему не удалось доказать достаточность этого критерия. Гаусс мимоходом утверждает («Disquisitiones Arithmeticae», Art. 303), что критерий Эйлера «легко доказать».]

## 8.2. Другая интерпретация циклического метода

Хотя определенные в предыдущем параграфе группы классов дивизоров и совпадают с группами, введенными Гауссом, внешне теория из § 8.1 совсем непохожа на гауссову теорию бинарных квадратичных форм. Мост между этими двумя теориями перебрасывает *циклический метод*. Существо дела отражает, по-видимому,

вычислительная техника циклического метода. При этом две изучаемые теории — теорию дивизоров квадратичных целых и теорию бинарных квадратичных форм — следует рассматривать как различные интерпретации тех типов задач, которые решаются при помощи этой вычислительной техники.

Древние индийцы пользовались циклическим методом задолго до того, как была изобретена столь утонченная теория, как теория дивизоров, и это обстоятельство ясно показывает, что циклический метод имеет и другие интерпретации, а не только как метод решения задачи, в которой требуется установить, является ли данный дивизор главным. Одна такая интерпретация, связанная

Таблица 8.2.1

$x^2 - 67y^2 = 1$	$x = 8y + z$
$-3y^2 + 16yz + z^2 = 1$	$y = 5z + a$
$6z^2 - 14za - 3a^2 = 1$	$z = 2a + b$
$-7a^2 + 10ab + 6b^2 = 1$	$a = b + c$
$9b^2 - 4bc - 7c^2 = 1$	$b = c + d$
$-2c^2 + 14cd + 9d^2 = 1$	$c = 7d + e$
$9d^2 - 14de - 2e^2 = 1$	$d = e + f$
$-7e^2 + 4ef + 9f^2 = 1$	$e = f + g$
$6f^2 - 10fg - 7g^2 = 1$	$f = 2g + h$
$-3g^2 + 14gh + 6h^2 = 1$	$g = 5h + i$
$h^2 - 16hi - 3i^2 = 1$	

с умножением двух уравнений вида  $a = x^2 - Dy^2$ , уже приводилась в § 1.9. Другая интерпретация будет рассмотрена ниже. По существу, она совпадает с подходом Броункера, Эйлера и Лагранжа, использующим непрерывные дроби. Почти без тени сомнения можно утверждать, что Гаусс был знаком с этим подходом в то время, когда он формулировал свою теорию.

В § 1.9 мы использовали циклический метод для того, чтобы найти решение  $x = 48\,842$ ,  $y = 5967$  уравнения

$x^2 = 67y^2 + 1$ . Вычисления, при помощи которых было найдено это решение, можно мотивировать следующим образом. Перепишем рассматриваемое уравнение в виде  $x^2 - 67y^2 = 1$ . Здесь  $x$  и  $y$  должны быть положительными целыми. Ясно, что  $x$  должно быть намного больше, чем  $y$ . В действительности  $x$  больше, чем  $8y$  (поскольку  $(8y)^2 - 67y^2 < 0$ ), но меньше, чем  $9y$  (поскольку  $(9y)^2 - 67y^2 > 1$ ). Определим  $z$  из равенства  $x = 8y + z$ ; тогда  $x > y > z > 0$ . Следовательно, данная задача эквивалентна задаче нахождения целых чисел  $y$  и  $z$ , удовлетворяющих уравнению  $(8y + z)^2 - 67y^2 = 1$ , т. е.  $-3y^2 + 16yz + z^2 = 1$ , и неравенствам  $y > z > 0$ . При этом мы не рассматриваем тривиальное решение  $y = 0$ ,  $z = 1$ . Уравнение  $x^2 - 67y^2 = 1$  дает информацию о частном при делении  $x$  на  $y$ ; точно так же новое уравнение  $-3y^2 + 16yz + z^2 = 1$  дает информацию о частном при делении  $y$  на  $z$ . При  $y = z$ ,  $2z$ ,  $3z$ ,  $4z$  или  $5z$  значение  $-3y^2 + 16yz + z^2$  отрицательно и поэтому слишком мало. Если же  $y \geq 6z$ , то это значение больше 1 и, следовательно, слишком велико. Таким образом,  $y = 5z + a$ , где  $z > a > 0$ , и данная задача эквивалентна урав-

нению  $-3(5z + a)^2 + 16(5z + a)z + z^2 = 1$ , т. е.  $6z^2 - 14za - 3a^2 = 1$ , где  $z > a > 0$ . Следуя этому методу, мы получим последовательность уравнений из табл. 8.2.1.

Легко найти решение последнего уравнения, удовлетворяющее условию  $h > i$ , а именно:  $h = 1, i = 0$ . Тогда решение предпоследнего уравнения равно  $g = 5h + i = 5, h = 1$ ; затем мы получаем решение уравнения, предшествующего предпоследнему:  $f = 2g + h = 11, g = 5$  и т. д. Такой процесс обратной подстановки приводит нас к искомому решению  $x = 48\,842, y = 5967$ .

Вычисления, которые требуются для составления табл. 8.2.1, в основном совпадают — хотя здесь они выступают в совершенно ином облике — с теми вычислениями, которые необходимо было произвести для нахождения последовательных значений  $a$  и  $r$  по образцу из гл. 7:

$$D = 67$$

$$\begin{array}{cccccccccccc} r = & 8 & 7 & 5 & 2 & 7 & 7 & 2 & 5 & 7 & 8 \\ a = & 1 & -3 & 6 & -7 & 9 & 2 & 9 & -7 & 6 & -3 & 1. \end{array}$$

Соответствие между этими двумя формами вычислений можно выразить в следующем виде: если  $a_i, a_{i+1}$  и  $a_{i+2}$  — три последовательных значения  $a$  в циклическом методе,  $r_i$  и  $r_{i+1}$  — промежуточные значения  $r$  и  $n_{i+1} = (r_i + r_{i+1})/a_{i+1}$ , то подстановка  $u = |n_{i+1}|v + w$  преобразует бинарную квадратичную форму  $a_{i+1}u^2 \pm 2r_i uv + a_i v^2$  в бинарную квадратичную форму  $a_{i+2}v^2 \mp 2r_{i+1}vw + a_{i+1}w^2$ , где знак среднего слагаемого в обеих квадратичных формах противоположен знаку первого слагаемого. Эту теорему, которая основывается здесь на простом сравнении приведенных выше двух вычислений, легко проверить алгебраически. Действительно, коэффициент при  $w^2$  в  $a_{i+1}(|n_{i+1}|v + w)^2 \pm 2r_i(|n_{i+1}|v + w)v + a_i v^2$ , очевидно, равен  $a_{i+1}$ . Коэффициент при  $vw$  равен  $2a_{i+1}|n_{i+1}| \pm 2r_i = (\operatorname{sgn} a_{i+1})(2r_i + 2r_{i+1}) \pm 2r_i = \mp 2r_{i+1}$ , где знак при  $r_i$  противоположен знаку  $a_{i+1}$ . Наконец, коэффициент при  $v^2$  равен  $a_{i+1}n_{i+1}^2 \pm 2r_i|n_{i+1}| + a_i$ . Если последнее выражение умножить на  $a_{i+1}$ , то оно превращается в  $(r_i + r_{i+1})^2 - 2r_i(r_i + r_{i+1}) + r_i^2 - D = r_{i+1}^2 - D = a_{i+1}a_{i+2}$ . Таким образом, как и утверждалось, данный коэффициент равен  $a_{i+2}$  (поскольку  $a_{i+1} \neq 0$ ).

Одной из первых задач теории бинарных квадратичных форм является задача нахождения *представлений* данного целого числа  $t$

<sup>1)</sup> *Формой* называется многочлен, все слагаемые которого имеют одинаковую степень. *Квадратичной формой* называется форма, для которой эта степень равна двум. *Бинарной квадратичной формой* называется квадратичная форма от двух переменных.

данной формой<sup>1)</sup>  $ax^2 + 2bxy + cy^2$ , т. е. нахождения при данных целых  $a, b, c$  и  $m$  таких целых  $x$  и  $y$ , что  $ax^2 + 2bxy + cy^2 = m$ . Приведенное выше решение задачи представления числа 1 бинарной квадратичной формой  $x^2 - 67y^2$  позволяет сделать вывод, что все бинарные квадратичные формы в табл. 8.2.1 эквивалентны в том смысле, что любое число, представимое одной из этих форм, представимо всеми этими формами, причем переход от представления одной из них к представлению другими совершается при помощи замен переменных, приведенных в правом столбце таблицы. Например, для того чтобы решить уравнение  $x^2 - 67y^2 = -2$ , можно заметить, что подстановка  $c = 1$  и  $d = 0$  в выражение  $-2c^2 + 14cd + 9d^2$  дает представление этой формой числа  $-2$ . Тогда  $b = c + d = 1$ ,  $a = b + c = 2$ ,  $z = 2a + b = 5$ ,  $y = 5z + a = 27$  и  $x = 8y + z = 221$  дает представление  $(221)^2 - 67(27)^2 = -2$ . Это приводит нас к еще одной трактовке циклического метода, а именно, к следующей.

Две бинарные квадратичные формы  $ax^2 + 2bxy + cy^2$  и  $a'u^2 + 2b'uv + c'v^2$  называются эквивалентными, если существует обратимая замена переменных с целыми коэффициентами, которая переводит одну форму в другую. Точнее, две формы называются эквивалентными, если существуют такие целые  $\alpha, \beta, \gamma, \delta$ , что  $\alpha\delta - \beta\gamma = \pm 1$  и подстановка  $x = \alpha u + \beta v$  и  $y = \gamma u + \delta v$  в  $ax^2 + 2bxy + cy^2$  дает  $a'u^2 + 2b'uv + c'v^2$ . Поскольку

$$ax^2 + 2bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

мы можем переформулировать это утверждение на языке  $2 \times 2$ -матриц в виде

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Здесь определитель  $\Delta = \alpha\delta - \beta\gamma$  замены координат равен  $\pm 1$ , поэтому матрица обратной замены

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \begin{pmatrix} \delta/\Delta & -\beta/\Delta \\ -\gamma/\Delta & \alpha/\Delta \end{pmatrix}$$

имеет целые элементы.

Таким образом, если  $a_i, a_{i+1}$  и  $a_{i+2}$  — три последовательных значения  $a$  в циклическом методе и  $r_i, r_{i+1}$  — промежуточные значения  $r$ , то бинарные квадратичные формы  $a_ix^2 + 2r_ixy + a_{i+1}y^2$  и  $a_{i+1}u^2 + 2r_{i+1}uv + a_{i+2}v^2$  эквивалентны. Это следует из приве-

<sup>1)</sup> Обратите внимание на то, что коэффициент при  $xy$  предполагается четным. Это сделано для согласования с обозначениями Гаусса. При решении уравнения  $ax^2 + bxy + cy^2 = m$  это не приводит к потере общности. Действительно, если  $b$  нечетно, то обе части уравнения можно удвоить.

денной выше теоремы, если заметить, что форма  $ax^2 + 2bxy + cy^2$  эквивалентна как  $au^2 - 2buv + cv^2$  ( $x = u, y = -v$ ), так и  $av^2 + 2buv + cu^2$  ( $x = v, y = u$ ). Эту эквивалентность можно записать в явном виде

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & n_{i+1} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}; \quad \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} n_{i+1} & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

где  $n_{i+1} = (r_i + r_{i+1})/a_{i+1}$ . Другими словами,

$$\begin{pmatrix} a_i & r_i \\ r_i & a_{i+1} \end{pmatrix} = \begin{pmatrix} n_{i+1} & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{i+1} & r_{i+1} \\ r_{i+1} & a_{i+2} \end{pmatrix} \begin{pmatrix} n_{i+1} & 1 \\ -1 & 0 \end{pmatrix}.$$

Так как определители  $a_i a_{i+1} - r_i^2 = -D$  и  $1 \cdot (a_{i+1} a_{i+2} - r_{i+1}^2) \times \times 1 = -D$  этих матриц равны, а обе матрицы симметричны, мы можем легко проверить последнее равенство, заметив, что последняя строка в правой части, как и требуется, равна  $a_{i+1} n_{i+1} - r_{i+1} = r_i$  и  $a_{i+1}$ .

Таким образом, циклический метод можно применять для быстрого построения эквивалентных форм и этим путем решать задачи нахождения представлений. Рассмотрим, например, задачу представления числа  $-3$  формой  $13x^2 + 6xy - 4y^2$ . Здесь  $D = 61$  и циклический метод дает

$$\begin{array}{cccccccc} r = & 3 & 5 & 4 & 6 & 4 & 5 & 7 \\ a = & 13 & -4 & 9 & -5 & 5 & -9 & 4 & -3. \end{array}$$

Последние три числа соответствуют форме  $4u^2 + 14uv - 3v^2$ , которая, очевидно, представляет  $-3$  (при  $u = 0, v = 1$ ). Согласно доказанной выше теореме, эквивалентность между этой формой и данной формой  $13x^2 + 6xy - 4y^2$ , задается в явном виде формулой

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$$

При  $u = 0, v = 1$  эта формула дает решение  $x = -37, y = -100$  первоначальной задачи.

Этот пример имеет несколько искусственный характер, поскольку данное число  $-3$  встречается в нижней строке при применении циклического метода к исходной форме. Более общий метод заключается в том, чтобы *построить* форму, которая очевидным образом представляет данное число, и попытаться использовать циклический метод для того, чтобы установить эквивалентность построенной формы данной форме.

Например, рассмотрим представление числа  $-217$  формой  $7x^2 - 6xy + y^2$ . При  $D = 2$  циклический метод дает эквивалентные формы

$$\begin{array}{cccc} -3 & 1 & 1 & \dots \\ 7 & 1 & -1 & 1 \dots \end{array}$$

Форма, которая очевидным образом представляет  $-217$ , имеет вид  $-217u^2 + 2div + ev^2$ , где числа  $d$  и  $e$  надлежит найти. Если найденные выше формы можно получить применением циклического метода к форме  $-217u^2 + 2div + ev^2$ , то  $d^2 - D = -217e$ , где  $D = 2$ . В частности,  $d^2 \equiv 2 \pmod{217}$ . Для решения этого сравнения можно следующим образом воспользоваться китайской теоремой об остатках. Имеем  $217 = 7 \cdot 31$ . Из сравнения  $d^2 \equiv 2 \pmod{7}$  следует, что  $d \equiv \pm 3 \pmod{7}$ . Сравнение по модулю 31 дает  $d \equiv \pm 8 \pmod{31}$ . Таким образом, получаются четыре возможных значения  $d \equiv \pm 39, \pm 101 \pmod{217}$ . Например, если  $d = 39$ , то  $e = -(d^2 - D)/217 = -7$ . Тогда циклический метод

$$\begin{array}{cccc} 39 & 3 & 1 & 1 \\ -217 & -7 & -1 & 1 \dots \end{array}$$

приводит эту форму к тем формам, которые мы получили выше. Запишем эти вычисления в обратном порядке и добавим полученную таблицу к таблице, найденной циклическим методом для формы  $7x^2 - 6xy + y^2$ :

$$\begin{array}{cccc} -3 & 1 & 3 & 39 \\ 7 & 1 & -1 & -7 \dots -217 \end{array}$$

Это показывает, что форма  $7x^2 - 6xy + y^2$  эквивалентна форме  $-7u^2 + 78uv - 217v^2$ , причем в явном виде эквивалентность задается равенством

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -6 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

При  $u = 0$  и  $v = 1$  последняя формула дает представление  $7 \times (-23)^2 - 6(-23)(-40) + (-40)^2 = -217$ .

Общий метод решения уравнения  $ax^2 + 2bxy + cy^2 = t$  представляет собой простое обобщение этого примера. Пусть  $D$  определено равенством  $b^2 - D = ac$ , т. е.  $D = b^2 - ac$ . Воспользуемся циклическим методом, взяв  $a$  и  $c$  в качестве первых двух значений  $a$ , а  $b$  — в качестве первого значения  $r$ . В конце концов <sup>1)</sup>

<sup>1)</sup> При этом предполагается, что  $D = b^2 - ac$  не является квадратом, так что  $r^2 - D \neq 0$ . Гаусс со свойственной ему обстоятельностью рассмотрел также случай, когда  $D$  — квадрат (*Disquisitiones Arithmeticae*, Art. 215). Однако найденное им в этом случае решение не использует ни циклического метода, ни группы классов; поэтому здесь оно не представляет для нас интереса.



это приведет нас к *периоду*, т. е. к повторению чисел, порождаемых циклическим методом. При данном  $m$  рассмотрим сравнение  $d^2 \equiv D \pmod{m}$ . Для любого решения  $d$  этого сравнения (все решения этого сравнения находятся за конечное число шагов) определим  $e$  равенством  $D = d^2 - em$  и рассмотрим бинарную квадратичную форму  $tu^2 + 2duv + ev^2$ . Применение циклического метода к этой форме также приводит к периоду. Если этот период совпадает с найденным выше периодом, то можно найти решение уравнения  $ax^2 + 2bxy + cy^2 = m$ . Действительно, в этом случае формы  $ax^2 + 2bxy + cy^2$  и  $tu^2 + 2duv + ev^2$  эквивалентны одной и той же форме, поэтому они эквивалентны друг другу. Фактически легко находятся явные формулы, задающие эту эквивалентность; поэтому искомое представление можно получить, просто положив  $u = 1, v = 0$ .

Можно показать, что этот метод всегда дает представление (при условии, что оно существует)<sup>1)</sup>. Точнее, если уравнение  $ax^2 + 2bxy + cy^2 = m$  имеет решение, то должно существовать по крайней мере одно решение  $d$  сравнения  $d^2 \equiv D \pmod{m}$ , обладающее тем свойством, что применение циклического метода к форме  $tu^2 + 2duv + ev^2$  (где  $e = (d^2 - D)/m$ ) дает тот же период, что и применение циклического метода к форме  $ax^2 + 2bxy + cy^2$ . Однако здесь мы скорее хотим показать ясную картину связи между циклическим методом и бинарными квадратичными формами, чем получить полное решение уравнения  $ax^2 + 2bxy + cy^2 = m$  (это решение см. в упр. 7 и 8 к § 8.4). Таким образом, циклический метод становится связующим звеном между теорией дивизоров и теорией бинарных квадратичных форм. Определяемое им соответствие между дивизорами и бинарными квадратичными формами является предметом следующего параграфа.

## Упражнения

1. Докажите, что замена переменных  $x' = ax + by, y' = cx + dy$  с целыми коэффициентами  $a, b, c, d$  обратима (т. е. обратная к ней замена также имеет целые коэффициенты) тогда и только тогда, когда определитель  $ad - bc$  равен  $\pm 1$ .

2. Используйте приведенный в основном тексте метод для нахождения двух существенно различных представлений  $x^2 + y^2 = 65$ .

<sup>1)</sup> Точнее, этот метод дает *собственное* представление  $ax^2 + 2bxy + cy^2 = m$ , т. е. представление, в котором  $x$  и  $y$  взаимно просты (при условии, что такое представление возможно). Несобственное представление, в котором  $x = dx', y = dy'$ , где  $d > 1$  и  $x', y'$  взаимно просты, существует, только если  $m$  делится на квадрат:  $m = d^2 m'$  и  $m'$  имеет собственное представление  $ax'^2 + 2bx'y' + cy'^2 = m'$  данной формой. Таким образом, если описанный выше метод не дает представления  $m$ , то следует выделить из  $m$  квадрат  $d^2$  и попытаться найти представление числа  $m/d^2$  данной формой. Если это также не удастся, то такого представления не существует. Доказательства этих утверждений рассмотрены в упр. 7 к § 8.4.

3. Используйте приведенный в основном тексте метод для нахождения представления числа 121 формой  $4x^2 + 2xy + 5y^2$ .

4. Найдите представление числа 23 формой  $15x^2 + 40xy + 27y^2$ .

5. Найдите представление числа 129 формой  $42x^2 + 118xy + 81y^2$ .

6. Найдите представление числа 91 формой  $x^2 + xy + y^2$ .

### 8.3. Соответствие между дивизорами и бинарными квадратичными формами

Для того чтобы установить связь между группами классов дивизоров, определенными в § 8.1, и группами, которые Гаусс ввел в своей теории бинарных квадратичных форм, необходимо установить связь между дивизорами и бинарными квадратичными формами. В простейшем случае, когда  $D$  свободно от квадратов и сравнимо с 2 или 3 по модулю 4, рассуждения из предыдущего параграфа ясно показывают, как это следует сделать.

Пусть  $D \not\equiv 1 \pmod{4}$  — целое число, свободное от квадратов. Предположим, что  $A$  — дивизор для квадратичных целых детерминанта  $D$ , причем  $A$  не делится ни на одно целое, большее 1. Тогда применение циклического метода к дивизору  $A$  равносильно применению этого метода к бинарной квадратичной форме  $ax^2 + 2bxy + cy^2$ , где  $a = N(A)$ ,  $b \equiv \sqrt{D} \pmod{A}$  и  $c = (b^2 - D)/a$  (с тем лишь исключением, что условие  $b \equiv \sqrt{D} \pmod{A}$  не определяет <sup>1)</sup>  $b$  однозначно, а определяет лишь класс  $b$  по модулю  $a$ ). Таким образом, можно определить отображение множества дивизоров, не делящихся ни на одно целое, большее 1, в множество квадратичных форм, удовлетворяющих условию  $b^2 - ac = D$ , выбирая  $b$  по правилам циклического метода. Точнее, рассмотрим класс вычетов по модулю  $a$ , элементы которого удовлетворяют сравнению  $b \equiv \sqrt{D} \pmod{A}$ . Если в этом классе найдется такой элемент  $b$ , что  $b^2 < D$ , то выберем в качестве  $b$  наибольший элемент, для которого  $b^2 < D$ . В противном случае в качестве  $b$  выберем элемент из этого класса с наименьшим значением  $|b|$  (если найдутся два таких элемента, выберем положительный).

Это отображение (некоторого) множества дивизоров квадратичных целых детерминанта  $D$  в (некоторое) множество бинарных квадратичных форм с  $b^2 - ac = D$  <sup>2)</sup> является взаимно однозначным. Легко найти обратное к нему отображение. Заданная бинарная квадратичная форма  $ax^2 + 2bxy + cy^2$  с  $b^2 - ac = D$  может получиться из дивизора  $A$ , только если  $a = N(A)$  и  $b \equiv \sqrt{D} \pmod{A}$ . Для того чтобы эта форма была образом некоторого дивизора  $A$ , при  $D < 0$  необходимо, чтобы  $a$  было больше нуля (поскольку при

<sup>1)</sup> Существует по крайней мере одно целое  $b$ , удовлетворяющее этому условию. Действительно, в § 7.4 доказано, что если  $A$  не делится ни на одно целое, большее 1, то  $\sqrt{D}$  сравним с некоторым целым по модулю  $A$ .

<sup>2)</sup> Гаусс называл  $b^2 - ac$  *детерминантом* бинарной квадратичной формы; мы будем следовать здесь этой терминологии.

$D < 0$  нормы дивизоров положительны; отсюда следует также, что  $c > 0$ ). Будем считать, что для рассматриваемых форм это необходимое условие выполнено. Тогда легко видеть, что такая форма определяет единственный дивизор  $A$  со свойствами  $a = N(A)$ ,  $b \equiv \sqrt{D} \pmod{A}$ . Действительно,  $b - \sqrt{D}$  не делится ни на одно целое, поэтому его дивизор является произведением простых дивизоров, в которое не входят дивизоры простых чисел, остающихся простыми в квадратичных целых детерминанта  $D$ . Кроме того, это произведение может содержать только один из двух простых множителей распадающегося простого числа. Таким образом, дивизор, который делит  $b - \sqrt{D}$ , полностью определяется своей нормой (что учитывает отсутствие или наличие множителя  $(-1, *)$  при  $D > 0$ ), и каждый делитель нормы  $N(b - \sqrt{D}) = b^2 - D = ac$  является нормой некоторого дивизора, делящего  $b - \sqrt{D}$  (при  $D < 0$  такой делитель должен быть положительным).

Согласно теореме из § 7.7, при этом соответствии *эквивалентные дивизоры соответствуют эквивалентным бинарным квадратичным формам*. Действительно, эта теорема показывает, что два эквивалентных дивизора могут быть приведены циклическим методом к одному и тому же дивизору. Кроме того, циклический метод преобразует бинарные квадратичные формы в эквивалентные бинарные квадратичные формы, поэтому формы, соответствующие эквивалентным дивизорам, эквивалентны одной и той же форме (полученной приведением каждого из дивизоров к его периоду) и, следовательно, эквивалентны друг другу.

Однако *обратное утверждение не обязательно верно*. Действительно, если  $A$  — дивизор, который не делится ни на одно целое, большее 1, и если  $ax^2 + 2bxy + cy^2$  — соответствующая бинарная квадратичная форма, то  $\bar{A}$  соответствует  $ax^2 - 2bxy + cy^2$  или эквивалентной ей форме (если по правилам циклического метода выбирается  $b' \equiv -b \pmod{a}$ , отличное от  $b' = -b$ ). Таким образом,  $A$  и  $\bar{A}$  соответствуют эквивалентным бинарным квадратичным формам (замена  $x \mapsto x, y \mapsto -y$  преобразует  $ax^2 + 2bxy + cy^2$  в  $ax^2 - 2bxy + cy^2$ ), хотя обычно дивизоры  $A$  и  $\bar{A}$  не эквивалентны. Однако Гаусс заметил, что *определение эквивалентности бинарных квадратичных форм не является достаточно ограничительным*; это замечание играет ключевую роль в его теории. Правильное определение эквивалентности бинарных квадратичных форм можно найти, если перевести на язык квадратичных форм определение эквивалентности дивизоров. Если две бинарные квадратичные формы соответствуют эквивалентным дивизорам, то каждую из них можно преобразовать циклическим методом к некоторой третьей форме. Это не только устанавливает эквивалентность исходных квадратичных форм, но и дает эквивалентность, которая пред-

ставляется как композиция преобразований вида

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & n_{i+1} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$$

и обратных к ним. Поскольку определитель каждого из этих преобразований равен  $+1$ , это показывает, что две данные формы должны быть эквивалентны относительно преобразования с определителем, равным  $+1$ .

**Определение.** Две бинарные квадратичные формы  $ax^2 + 2bxy + cy^2$  и  $a'u^2 + 2b'uv + c'v^2$  называются *собственно эквивалентными*, если существует замена координат  $x = \alpha u + \beta v$ ,  $y = \gamma u + \delta v$  с  $\alpha\delta - \beta\gamma = 1$ , которая преобразует одну из форм в другую. Иначе говоря, формы *собственно эквивалентны*, если существуют целые  $\alpha, \beta, \gamma, \delta$ , удовлетворяющие условиям

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{и} \quad \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1. \quad (1)$$

Тогда *эквивалентные дивизоры соответствуют собственно эквивалентным формам*. Как будет показано ниже, справедлива и обратная теорема, а именно *если формы, соответствующие двум дивизорам, собственно эквивалентны, то дивизоры эквивалентны друг другу*.

Такое различие эквивалентности и собственной эквивалентности форм казалось Куммеру искусственным. Он надеялся, что его теория идеальных комплексных чисел сумеет объяснить это различие, показав, что формы  $ax^2 + 2bxy + cy^2$  и  $ax^2 - 2bxy + cy^2$  представляют собой «не что иное, как два идеальных делителя одного и того же числа» [К7, стр. 324]. Куммер ничего не говорит о том, каким образом формы  $ax^2 + 2bxy + cy^2$  и  $ax^2 - 2bxy + cy^2$  представляют дивизоры (идеальные числа), но, без сомнения, он имел в виду нечто похожее на приведенное выше соответствие, при котором сопряженные дивизоры отвечают формам  $ax^2 \pm \pm 2bxy + cy^2$  или по крайней мере *собственно эквивалентным* им формам.

Подводя итоги, можно сказать, что существует естественное взаимно однозначное соответствие между классами эквивалентности дивизоров квадратичных целых детерминанта  $D$  и классами *собственной* эквивалентности бинарных квадратичных форм с детерминантом  $D$  (здесь мы предполагаем, что  $D \not\equiv 1 \pmod{4}$ ,  $D$  свободно от квадратов, и при  $D < 0$  рассматриваем лишь формы с положительными  $a$  и  $c$ ). В оставшейся части этого параграфа мы должны доказать, что если  $D$  не свободно от квадратов или  $D \equiv \equiv 1 \pmod{4}$ , то классы *собственной* эквивалентности форм по-прежнему находятся в естественном взаимно однозначном соот-

ветствии с классами эквивалентности дивизоров (здесь обычная эквивалентность заменяется эквивалентностью относительно подходящего порядка, определенной в § 8.1).

В определенном выше соответствии бинарная квадратичная форма  $ax^2 + 2bxy + cy^2$  отвечает дивизору, который делит  $b - \sqrt{b^2 - ac}$  и имеет норму  $a$ . Здесь предполагается, что  $D = b^2 - ac$  свободно от квадратов,  $D \not\equiv 1 \pmod{4}$  и, кроме того,  $a > 0$  при  $D < 0$ . Однако то же самое правило можно использовать во всех случаях, когда  $a, b, c$  — такие числа, что два условия: « $A$  делит  $b - \sqrt{b^2 - ac}$ » и « $N(A) = a$ » — определяют единственный дивизор  $A$ . Нетрудно найти естественные условия на числа  $a, b, c$ , гарантирующие, что эти числа будут обладать требуемым свойством, если воспользоваться опытом, который мы приобрели в § 8.1. Этот опыт подсказывает, что при обращении с квадратичными целыми  $x + y\sqrt{D}$  ( $x, y$  — целые) естественно рассматривать лишь дивизоры, взаимно простые с индексом  $s$  порядка  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$ . Индекс  $s$  равен  $t$ , если  $D = t^2 D'$ , где  $D'$  свободно от квадратов и  $D' \not\equiv 1 \pmod{4}$ , и равен  $2t$ , если  $D = t^2 D'$ , где  $D'$  свободно от квадратов и  $D' \equiv 1 \pmod{4}$ . Это заставляет нас потребовать, чтобы в квадратичной форме  $ax^2 + 2bxy + cy^2$  коэффициент  $a$  был взаимно прост с наибольшим квадратом, на который делится  $b^2 - ac$ , и, кроме того, при  $b^2 - ac \equiv 1 \pmod{4}$  коэффициент  $a$  должен быть нечетным (взаимно простым с 2). (Если  $b^2 - ac = t^2 D'$ , то из сравнения  $b^2 - ac \equiv 1 \pmod{4}$  следует, что  $t$  нечетно и  $D' \equiv 1 \pmod{4}$ . Обратно, если  $D' \equiv 1 \pmod{4}$ , то либо  $t$  четно (и уже первое условие требует нечетности  $a$ ), либо  $t$  нечетно и  $b^2 - ac \equiv 1 \pmod{4}$ .) Кроме того, если  $b^2 - ac < 0$ , то неравенство  $a > 0$  является необходимым условием для того, чтобы  $a$  было нормой дивизора  $A$ .

**Теорема.** Пусть  $a, b, c$  — целые числа; предположим, что  $b^2 - ac = t^2 D'$ , где  $D'$  свободно от квадратов. Если  $a$  взаимно просто с  $t$  (и  $a$  нечетно при  $b^2 - ac \equiv 1 \pmod{4}$ ) и если  $a > 0$  при  $b^2 - ac < 0$ , то условия  $N(A) = a$  и  $b \equiv \sqrt{D} \pmod{A}$  определяют единственный дивизор  $A$  для квадратичных целых детерминанта  $D'$ .

1) Пусть  $a', b', c'$  — другая тройка целых чисел. Предположим, что  $(b')^2 - a'c' = b^2 - ac$ , и пусть  $a'$  удовлетворяет тем же самым условиям, что и  $a$ . Тогда бинарные квадратичные формы  $ax^2 + 2bxy + cy^2$  и  $a'x^2 + 2b'xy + c'y^2$  являются собственно эквивалентными в том и только в том случае, когда соответствующие дивизоры эквивалентны относительно порядка  $\{x + y\sqrt{D} : x, y \text{ — целые}, D = b^2 - ac\}$ .

2) Если  $ax^2 + 2bxy + cy^2$  — квадратичная форма, для которой не выполняются приведенные выше условия на  $a$ , то необходимые и достаточные условия для того, чтобы  $ax^2 + 2bxy + cy^2$  была



собственно эквивалентна бинарной квадратичной форме  $a'x^2 + 2b'xy + c'y^2$ , где  $a'$  удовлетворяет соответствующим условиям, заключаются в том, что целые  $a$ ,  $2b$  и  $c$  не должны иметь общий делитель, больший 1, и  $a$  должно быть положительным при  $b^2 - ac < 0$ .

Гаусс называл бинарную квадратичную форму  $ax^2 + 2bxy + cy^2$  собственно примитивной, если  $a$ ,  $2b$  и  $c$  не имеют общих делителей, больших 1. (Форма называется примитивной, если  $a$ ,  $b$ ,  $c$  не имеют общих делителей, больших 1.) Из утверждения 2) следует, что любая форма, собственно эквивалентная собственно примитивной форме, собственно примитивна. Поэтому имеет смысл говорить о собственно примитивных классах собственной эквивалентности форм. Аналогично, если  $b^2 - ac < 0$  и  $a > 0$ , то каждая форма, собственно эквивалентная  $ax^2 + 2bxy + cy^2$ , обладает теми же самыми свойствами. Гаусс называл такую форму положительной. (В современной терминологии ее называют положительно определенной.) Поэтому имеет смысл говорить о положительных классах собственной эквивалентности форм. Вторая часть сформулированной теоремы утверждает, что собственно примитивный и при  $D < 0$  положительный класс собственной эквивалентности форм содержит формы, соответствующие дивизорам. В первой части утверждается, что различные формы, принадлежащие одному классу, соответствуют эквивалентным дивизорам. Следовательно, эта теорема показывает, что существует отображение из множества классов собственной эквивалентности форм (собственно примитивных, и при  $D < 0$  положительных) в классы эквивалентности дивизоров (для квадратичных целых порядка  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$ ). Это отображение является взаимно однозначным. Действительно, согласно первому утверждению теоремы, формы, соответствующие эквивалентным дивизорам, должны быть собственно эквивалентны. Кроме того, оно отображает классы форм на всю группу классов дивизоров, поскольку каждый класс из этой группы содержит дивизор  $A$ , который взаимно прост с индексом порядка и не делится ни на одно целое, большее 1, а такой дивизор  $A$  является образом квадратичной формы  $ax^2 + 2bxy + cy^2$ , где  $a = N(A)$ ,  $b \equiv \sqrt{D} \pmod{A}$ ,  $c = (b^2 - D)/a$ . Таким образом, эта теорема устанавливает взаимно однозначное соответствие между элементами группы классов дивизоров порядка  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$  и классами собственной эквивалентности бинарных квадратичных форм  $ax^2 + 2bxy + cy^2$ , которые имеют детерминант  $D$ , являются собственно примитивными и при  $D < 0$  положительными. Поэтому данная теорема устанавливает связь между теориями Куммера и Гаусса. Оставшаяся часть параграфа посвящена доказательству теоремы.



**Доказательство.** Пусть  $a, b, c$  удовлетворяют условиям, сформулированным в начале теоремы. Тогда  $b - \sqrt{D} = b - t\sqrt{D'}$  является квадратичным целым детерминанта  $D'$  и его норма равна  $b^2 - D = ac$ . Если  $p$  — произвольный простой делитель  $a$ , то  $p$  не делит  $b - t\sqrt{D'}$ . (Действительно,  $a$  взаимно просто с  $t$ , поэтому  $p$  не делит  $t$ ; если  $p = 2$ , то  $t$  должно быть нечетным и  $b^2 - ac \not\equiv 1 \pmod{4}$ , т. е. 2 не делит  $b - t\sqrt{D'}$ .) Следовательно,  $p$  не остается простым; если  $p$  разветвляется, то его простой дивизор делит  $b - \sqrt{D}$  с кратностью точно 1, если же  $p$  распадается, то только один из двух его простых дивизоров делит  $b - \sqrt{D}$ . Таким образом,  $b - \sqrt{D}$  делится на один, и только на один, дивизор с нормой  $a$ . Этот дивизор совпадает с дивизором  $A$  из первой части теоремы.

Сначала мы докажем второе утверждение теоремы. Если некоторое нечетное простое делит  $a, 2b$  и  $c$ , то оно делит  $a, b, c$ . Тогда из определения собственной эквивалентности следует, что оно делит  $a', b', c'$  для любой формы  $a'x^2 + 2b'xy + c'y^2$ , эквивалентной данной форме. Поскольку квадрат этого простого делит  $D = b^2 - ac = t^2D'$ , оно делит как  $a'$ , так и  $t$ , и  $a'$  не обладает требуемыми свойствами. Если 2 делит  $a, 2b$  и  $c$ , то  $a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$  — четное число и либо  $b^2 - ac \equiv 0 \pmod{4}$  (при четном  $b$ ), либо  $b^2 - ac \equiv 1 \pmod{4}$  (при нечетном  $b$ ). В любом случае  $a'$  не обладает нужными свойствами. Наконец, если  $a < 0$  и  $b^2 - ac < 0$ , то  $a' = a^{-1}[(a\alpha + b\gamma)^2 - (b^2 - ac)\gamma^2] < 0$  и  $a'$  не удовлетворяет требованиям теоремы. Это показывает, что данные условия необходимы для того, чтобы существовала форма  $a'x^2 + 2b'xy + c'y^2$  с нужными свойствами.

Для доказательства достаточности этих условий заметим прежде всего, что, как показывает приведенное выше рассуждение, если  $a > 0$  и  $b^2 - ac < 0$ , то  $a' > 0$ . Остается лишь доказать, что если  $a, 2b, c$  взаимно просты, то существует форма, собственно эквивалентная данной, в которой  $a'$  взаимно просто с  $t$ , а если  $b^2 - ac \equiv 1 \pmod{4}$ , то  $a'$  нечетно. Гаусс (*Disquisitiones Arithmeticae*, Art. 228) не только доказал это утверждение; он показал также, что если  $a, 2b, c$  взаимно просты и  $k$  — произвольное целое, то существует форма, собственно эквивалентная данной, в которой  $a'$  взаимно просто с  $k$ . Для того чтобы это доказать, обозначим через  $\alpha$  произведение всех простых  $p$ , которые делят  $k$ , но не делят  $c$ , и пусть  $\gamma$  — произведение простых  $p$ , которые делят  $k$  и  $c$ , но не делят  $a$ . (Пустое произведение равно 1, т. е. если нет простых, удовлетворяющих приведенным требованиям, то «произведение» считается равным 1.) Тогда  $\alpha$  и  $\gamma$  взаимно просты и существует такое целое  $\delta$ , что  $\delta\alpha \equiv 1 \pmod{\gamma}$ . Положим  $\beta = (\alpha\delta - 1)/\gamma$ . Тогда  $\alpha\delta - \beta\gamma = 1$  и равенство (1) определяет форму, собственно эквивалентную  $ax^2 + 2bxy + cy^2$ , в которой  $a' = a\alpha^2 + 2b\alpha\gamma +$

$+cy^2$ . Мы должны показать, что  $a'$  взаимно просто с  $k$ . Если  $p$  — простой делитель  $k$ , который не делит  $c$ , то он делит  $\alpha$ , но не делит  $\gamma$ ; поэтому такое  $p$  не делит  $a'$ . Если  $p$  — простой делитель  $k$ , который делит  $c$ , но не делит  $a$ , то он делит  $\gamma$ , но не делит  $\alpha$ , а потому не делит и  $a'$ . Наконец, если  $p$  — простой делитель  $k$ , который делит как  $a$ , так и  $c$ , то он не делит ни  $\alpha$ , ни  $\gamma$ , ни  $2b$  (поскольку  $a, 2b, c$  взаимно просты); следовательно, он не делит  $a'$ . Таким образом,  $a'$  взаимно просто с  $k$ , что и требовалось показать.

Для доказательства утверждения 1) предположим, что  $ax^2 + 2bxy + cy^2$  и  $a'x^2 + 2b'xy + c'y^2$  — две формы с детерминантом  $D = t^2D'$ , в которых  $a$  и  $a'$  удовлетворяют требуемым условиям. Тогда они отвечают дивизорам  $A$  и  $A'$  соответственно. Прежде всего мы докажем, что если  $A$  и  $A'$  эквивалентны как дивизоры порядка  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$ , то эти формы собственно эквивалентны. Дивизор  $A'\bar{A}'$  — главный, поэтому из определения эквивалентности следует, что существует принадлежащий данному порядку элемент  $u + v\sqrt{D}$  с дивизором  $A\bar{A}'$ . Тогда умножение на  $u + v\sqrt{D}$  с последующим делением на  $a'$  переводит элементы данного порядка, делящиеся на  $A'$ , в элементы из этого порядка, делящиеся на  $A$ . Далее, элемент  $z + w\sqrt{D}$  из данного порядка делится на  $A'$  тогда и только тогда, когда  $z + wb' - w(b' - \sqrt{D})$  делится на  $A'$ . Последнее справедливо в том и только в том случае, когда  $z + wb' \equiv 0 \pmod{a'}$ . Другими словами, элемент  $z + w\sqrt{D}$  делится на  $A'$  тогда и только тогда, когда он имеет вид  $a'x + (b' - \sqrt{D})y$  (где  $x = (z + wb')/a'$ ,  $y = -w$ ). Аналогично, элемент  $z + w\sqrt{D}$  из данного порядка делится на  $A$  тогда и только тогда, когда он имеет вид  $ax + (b - \sqrt{D})y$  с целыми  $x$  и  $y$ . Тогда, как и в § 7.7, умножение на  $u + v\sqrt{D}$  с последующим делением на  $a'$  переводит  $a'x + (b' - \sqrt{D})y$  в  $ax' + (b - \sqrt{D})y'$ , где  $x' = \alpha x + \beta y$ ,  $y' = \gamma x + \delta y$  и

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \frac{u+vb}{a} & \frac{b'u - Dv - bu + bb'v}{aa'} \\ -v & \frac{u - vb'}{a'} \end{pmatrix}. \quad (2)$$

Композиция умножения на  $u + v\sqrt{D}$  с последующим делением на  $a'$  и умножения на  $u - v\sqrt{D}$  с последующим делением на  $a$  является тождественным отображением  $a'x + (b' - \sqrt{D})y \mapsto a'x + (b' - \sqrt{D})y$  (норма  $u + v\sqrt{D}$  равна  $aa'$ ); поэтому матрицу (2) можно обратить, заменяя  $u + v\sqrt{D}$  на  $u - v\sqrt{D}$  и меняя местами  $A$  и  $A'$ . Так как при этом  $\alpha$  и  $\delta$  меняются местами и знаки при  $\beta$  и  $\gamma$  заменяются на противоположные, то определитель матрицы (2) равен 1. Поэтому для доказательства собственной эквивалентности

этих форм достаточно доказать, что выполняется первое из равенств (1). Это можно сделать прямым вычислением:

$$\begin{aligned}
 a\alpha^2 + 2b\alpha\gamma + c\gamma^2 &= a^{-1} [(u + vb)^2 + 2b(u + vb)(-v) + acv^2] = \\
 &= a^{-1} [u^2 + v^2(b^2 - 2b^2 + ac)] = a^{-1} [aa'] = a'; \\
 a\alpha\beta + b\alpha\delta + b\beta\gamma + c\gamma\delta &= a\alpha\beta + b\alpha\delta + b(\alpha\delta - 1) + c\gamma\delta = \\
 &= -b + (aa')^{-1} [(u + vb)(b'u - Dv - bu + bb'v) + \\
 &\quad + 2b(u + vb)(u - vb') + ac(-v)(u - vb')] = \\
 &= -b + (aa')^{-1} [u^2(b' - b + 2b) + \\
 &\quad + uv(-D + bb' + bb' - b^2 + 2b^2 + 2bb' - ac) + \\
 &\quad + v^2(-bD + b^2b' - 2b^2b' + acb')] = \\
 &= -b + (aa')^{-1} [(b + b')u^2 - (b + b')Dv^2] = \\
 &= -b + (b + b') = b'.
 \end{aligned}$$

Тогда, как и требуется,  $c'' = \alpha\beta^2 + 2b\beta\delta + c\delta^2$  равно  $c'$ . Действительно, согласно предположению,  $b^2 - ac = D = b'^2 - a'c'$  и из (1) и уже доказанных утверждений следует, что  $b^2 - ac = b'^2 - a'c''$ . Так как  $a' \neq 0$ , то мы получаем отсюда, что  $c'' = c'$ .

Наконец, предположим, что данные формы собственно эквивалентны. Мы должны доказать, что тогда эквивалентны и дивизоры, или, что то же самое, что существует элемент  $u + v\sqrt{D}$  с дивизором  $A\bar{A}'$ . Проведенное выше рассуждение наводит на мысль положить  $v = -\gamma$  и  $u = \alpha a + \gamma b$  (из  $\alpha = (u + vb)/a$ ) или  $u = \delta a' - \gamma b'$  (из  $\delta = (u - vb')/a'$ ). Эти два определения  $u$  совпадают. Действительно, согласно (1),

$$\begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}; \quad (3)$$

отсюда следует, что  $\delta a' - \gamma b' = a\alpha + b\gamma$ . При таких определениях  $u$  и  $v$  имеем  $u + v\sqrt{D} = \alpha a + \gamma(b - \sqrt{D}) = \delta a' - \gamma(b' + \sqrt{D})$ , что, очевидно, делится на  $A$  и  $\bar{A}'$ . Норма  $u + v\sqrt{D}$  равна  $(a\alpha + b\gamma)^2 - D\gamma^2 = a[a\alpha^2 + 2b\alpha\gamma + c\gamma^2] = aa'$ . Если  $a$  и  $a'$  взаимно просты, этого достаточно для доказательства того, что дивизор  $u + v\sqrt{D}$  равен  $\bar{A}'A$ , а следовательно, и эквивалентности дивизоров  $A \sim A'$ , что и требовалось доказать. Если  $a$  и  $a'$  не взаимно просты, то метод, использованный при доказательстве второй части этой теоремы, показывает, что существует третья форма  $a''x^2 + 2b''xy + c''y^2$ , собственно эквивалентная обеим данным формам, в которой  $a''$  взаимно просто как с  $a$  и  $a'$ , так и с  $t$ . Если  $A''$  — соответствующий дивизор, то было показано, что  $A \sim A''$  и  $A' \sim A''$ . Таким образом,  $A \sim A'$ , и доказательство теоремы завершено.

## Упражнения

Для каждого из следующих детерминантов найдите одну бинарную квадратичную форму из каждого собственно примитивного класса собственной эквивалентности.

1.  $D = 67$ .
2.  $D = -165$  (включите отрицательные классы собственной эквивалентности).
3.  $D = 79$ .
4.  $D = -161$ .
5.  $D = -11$  (см. упр. 1 к § 8.1).
6.  $D = 18$  (см. упр. 6 к § 8.1).

## 8.4. Классификация форм

Для вычисления групп классов дивизоров, определенных в § 8.1, необходимо научиться устанавливать, являются ли два данных дивизора  $A$  и  $A'$  эквивалентными (конечно, при условии, что они взаимно просты с индексом  $s$  рассматриваемого порядка). Теорема из предыдущего параграфа показывает, что эту задачу можно свести к задаче установления собственной эквивалентности двух данных бинарных квадратичных форм. В случае  $s = 1$  мы решили эту задачу (правда, в терминах дивизоров, а не бинарных квадратичных форм) в гл. 7 при помощи циклического метода. При  $s > 1$  можно по-прежнему решать эту задачу циклическим методом. Однако применение циклического метода к дивизору, взаимно простому с  $s$ , не обязательно дает дивизор, взаимно простой с  $s$ , поэтому естественнее описывать решение в терминах бинарных квадратичных форм, а не дивизоров. При такой модификации терминологии теорема и ее доказательство, по существу, совпадают с соответствующими теоремой и доказательством из гл. 7.

**Теорема.** Пусть  $a_0x^2 + 2r_0xy + a_1y^2$  — данная бинарная квадратичная форма детерминанта  $r_0^2 - a_0a_1 = D$ , не являющегося квадратом. Определим две последовательности целых чисел  $a_0, a_1, a_2, \dots$  и  $r_0, r_1, r_2, \dots$  следующим образом. Если даны  $r_i$  и  $a_{i+1}$ , то  $r_{i+1}$  является решением сравнения  $r_i + r_{i+1} \equiv \equiv 0 \pmod{a_{i+1}}$ . Точнее, если это сравнение имеет решения  $r_{i+1}$ , для которых  $r_{i+1}^2 < D$ , то мы выбираем в качестве  $r_{i+1}$  наибольшее решение этого сравнения, удовлетворяющее условию  $r_{i+1}^2 < D$ . В противном случае в качестве  $r_{i+1}$  мы выбираем решение этого сравнения с наименьшим  $|r_{i+1}|$  (если таких решений два, то мы выберем положительное  $r_{i+1}$ ). Если даны  $a_i$  и  $r_i$ , то  $a_{i+1}$  определено условием:  $a_{i+1} = (r_i^2 - D)/a_i$ . Тогда все бинарные квадратичные формы  $a_ix^2 + 2r_ixy + a_{i+1}y^2$  собственно эквивалентны исходной форме  $a_0x^2 + 2r_0xy + a_1y^2$ . Кроме того, начиная с некоторого места, эти формы повторяются. Цикл повторяющихся форм называется периодом данной формы. Две бинарные квадратичные формы

*являются собственно эквивалентными тогда и только тогда, когда их периоды совпадают.*

Эта теорема является ключевой в классификации бинарных квадратичных форм. Ее доказательству посвящена оставшаяся часть этого параграфа. Коротко говоря, это доказательство в точности совпадает с доказательством из гл. 7 — мы должны лишь перевести его с языка теории дивизоров на язык теории бинарных квадратичных форм. Предположение о том, что  $D$  свободно от квадратов, в доказательстве из гл. 7 вообще не использовалось; мы пользовались им только для определения соответствия между формами и дивизорами.

В приведенной выше формулировке теоремы речь идет только о бинарных квадратичных формах, среднее слагаемое которых четно. Однако в следующем ниже доказательстве *мы будем рассматривать также и случай полуцелого  $r_0$* . Тогда, как и в гл. 7, вся последовательность  $r_i$ , порожденная циклическим методом, состоит из полуцелых чисел. При этом мы должны несколько изменить обозначения из гл. 7: в качестве  $D$  мы всегда будем брать  $b^2 - ac$ , так что если  $b$  — полуцелое, то  $D$  будет  $1/4$  целого, сравнимого с 1 по модулю 4. Тогда во всех случаях  $b - \sqrt{D}$  будет квадратичным целым.

Если  $a_0$ ,  $r_0$  и  $a_1$  имеют общий делитель, то он делит все следующие значения  $r$  и  $a$ . Форма  $a'_0x^2 + 2r'_0xy + a'_1y^2$  может быть эквивалентна исходной форме, только если  $a'_0$ ,  $r'_0$  и  $a'_1$  делятся на общий делитель  $a_0$ ,  $r_0$  и  $a_1$ . Следовательно, доказательство теоремы сводится к случаю, когда  $a_0$ ,  $r_0$  и  $a_1$  не имеют общих делителей. Кроме того, если  $a_0$ ,  $2r_0$  и  $a_1$  — четные целые, то  $r_0$  будет целым, и мы можем числа, получающиеся в циклическом методе, сократить на 2 (поскольку  $r_0$  может быть полуцелым). Следовательно, *общий случай сводится к случаю собственно примитивной формы  $a_0x^2 + 2r_0xy + a_1y^2$* . Это позволяет нам в следующем доказательстве предположить, что все формы  $a_ix^2 + 2r_ixy + a_{i+1}y^2$  являются собственно примитивными.

**Доказательство.** Согласно принципу бесконечного спуска, коэффициенты  $a_i$ ,  $a_{i+1}$ , удовлетворяющие неравенству  $|a_i| \leq |a_{i+1}|$ , должны встречаться бесконечно часто. Для таких коэффициентов  $|a_i|^2 \leq |a_ia_{i+1}| \leq r_i^2 + |D|$ . Согласно определению,  $r_i$  удовлетворяет одному из неравенств:  $r_i^2 < D$  или  $|r_i| \leq |a_i|/2$ . Это показывает, что такие  $a_i$  и соответствующие  $r_i$  могут принимать только конечное число значений ( $a_i^2 \leq 2|D|$  или  $a_i^2 \leq 1/4a_i^2 + |D|$ ,  $|a_i| \leq 2\sqrt{|D|/3}$ ). Следовательно, тройки целых чисел  $(a_i, r_i, a_{i+1})$  могут принимать только конечное число значений, для которых  $|a_i| \leq |a_{i+1}|$ . Таким образом, некоторая тройка должна встретиться в нашей последовательности дважды. Однако каждая тройка однозначно определяет следующую за ней



тройку, поэтому все формы, следующие за формой, которая дважды встречается в построенной последовательности, должны циклически повторяться *ad infinitum*.

В § 8.2 было показано, что каждая форма собственно эквивалентна следующей за ней форме из полученной последовательности. Следовательно, все формы в этой последовательности собственно эквивалентны исходной форме. Очевидно, что две формы с одним и тем же периодом собственно эквивалентны. Суть доказываемой теоремы состоит в том, что *если две формы собственно эквивалентны, то они имеют один и тот же период*.

Назовем форму *приведенной*, если она принадлежит своему периоду, т. е. если применение к этой форме циклического метода снова возвращает нас к ней. Каждая форма собственно эквивалентна приведенной форме с тем же самым периодом. Следовательно, мы должны доказать, что *если две приведенные формы собственно эквивалентны, то каждая из них принадлежит периоду другой из этих форм*.

При  $D < 0$  можно доказать это утверждение следующим образом <sup>1)</sup>. Не ограничивая общности, можно считать, что данные формы  $ax^2 + 2bxy + cy^2$  и  $a'x^2 + 2b'xy + c'y^2$  не только приведены, но и их коэффициенты удовлетворяют неравенствам  $|a| \leq |c|$ ,  $|a'| \leq |c'|$ . Действительно, каждый период содержит такую форму. Мы должны доказать, что если выполняются условия

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}; \quad \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1, \quad (1)$$

$a'$  также  $D = b^2 - ac < 0$ ,  $|a| \leq |c|$  и  $|a'| \leq |c'|$ , то две соответствующие формы принадлежат одному и тому же периоду. Так как  $aa' = a(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) = (a\alpha + b\gamma)^2 - D\gamma^2 \geq \geq |D|\gamma^2 \geq 0$  и  $a, a'$  отличны от нуля (в противном случае  $D = = b^2 - ac = b^2 \geq 0$  вопреки предположению), то  $aa' > 0$ . Следовательно,  $a$  и  $a'$  имеют одинаковые знаки. При необходимости изменяя эти знаки на противоположные, можно предположить, что  $a$  и  $a'$  — положительные числа. Из неравенства  $b^2 - ac = = D < 0$  следует, что  $c > 0$ . Аналогично,  $c' > 0$ . Так как  $|b| \leq \leq a/2$ ,  $a \leq c$ , то  $b^2 - ac = D$ ,  $a^2 \leq ac = b^2 + |D| \leq \leq 1/4 a^2 + + |D|$ ,  $3/4 a^2 \leq |D|$ ,  $a \leq 2\sqrt{|D|/3}$  и, аналогично,  $a' \leq \leq 2\sqrt{|D|/3}$ . Таким образом, из приведенного выше неравенства  $aa' \geq |D|\gamma^2$  следует, что  $4/3 |D| \geq |D|\gamma^2$  и  $\gamma^2 = 0$  или  $1$ .

*Случай 1.* Если  $\gamma^2 = 0$ , то  $\alpha\delta = 1$ ,  $\alpha = \delta = \pm 1$ ,  $a' = a\alpha^2 + + 2b\alpha\gamma + c\gamma^2 = a$  и  $b' = a\alpha\beta + b\alpha\delta + b\beta\gamma + c\gamma\delta = a\alpha\beta + b$ . Отсюда следует, что  $b \equiv b' \pmod{a}$ . Так как  $|b| < a/2$  или  $b =$

<sup>1)</sup> Сравните это доказательство с соответствующим доказательством из § 7.7. См. также § 65 из «Лекций по теории чисел» Дирихле [D7].



$= a/2$  и  $|b'| < a'/2 = a/2$  или  $b' = a/2$ , то из условия  $b \equiv b' \pmod{a}$  следует, что  $b = b'$ . Тогда  $c = c'$  и соответствующие формы совпадают.

*Случай 2.* Если  $\gamma^2 = 1$ , то, заменяя при необходимости  $\alpha, \beta, \gamma, \delta$  на  $-\alpha, -\beta, -\gamma, -\delta$ , можно предположить, что  $\gamma = 1$ . Тогда  $aa' = (a\alpha + b\gamma)^2 - D\gamma^2 = r^2 - D$ , где  $r = a\alpha + b \equiv b \pmod{a}$ . Поэтому, согласно выбору  $b$ ,  $|r| \geq |b|$ ,  $a \leq c = (b^2 - D)/a \leq (r^2 - D)/a = aa'/a = a'$ . Аналогично,  $aa' = (a'\delta - b'\gamma)^2 - D\gamma^2 = (r')^2 - D$ , где  $r' = a'\delta - b' \equiv -b' \pmod{a'}$ . Тогда  $|r'| \geq |b'|$  и  $a' \leq c' = [(b')^2 - D]/a' \leq [(r')^2 - D]/a' = a$ . Следовательно,  $a = c = a' = c'$ . Значит,  $b^2 = D + ac = D + a'c' = (b')^2$  и  $b = \pm b'$ . Если  $b = b'$ , то данные формы совпадают. Если  $b = -b'$ , то  $b \neq a/2$  (так как  $b' \neq -a/2$ ), и потому  $|b| < a/2$ . Следовательно, применение циклического метода к любой из этих форм дает вторую из них. Поэтому они принадлежат одному и тому же периоду, что и требовалось показать. Это завершает доказательство при  $D < 0$ .

При  $D > 0$  доказательство этой теоремы сложнее. Основным средством будет теорема из § 7.7 о разложениях вида

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} = \pm \begin{pmatrix} n_j & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} n_{j-1} & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_1 & 1 \\ -1 & 0 \end{pmatrix}, \quad (2)$$

где целые  $n_1, n_2, \dots, n_j$  образуют знакочередующуюся последовательность. Фактически все доказательство представляет собой прямую модификацию доказательства для случая  $s = 1$  из § 7.7.

Предположим, что  $M$  — такая целочисленная  $2 \times 2$ -матрица, что

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = M^t \begin{pmatrix} a & b \\ b & c \end{pmatrix} M; \quad \det M = 1,$$

где  $a'x^2 + 2b'xy + c'y^2$  и  $ax^2 + 2bxy + cy^2$  — две приведенные формы и  $M^t$  — матрица, транспонированная к  $M$ . На первом этапе мы должны доказать, что без ограничения общности можно заменить  $M$  на матрицу, которая имеет разложение вида (2). Для этого заметим прежде всего, что применение циклического метода к приведенной форме  $ax^2 + 2bxy + cy^2$  задает собственную эквивалентность этой формы с собой:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} = E_1^t \begin{pmatrix} a & b \\ b & c \end{pmatrix} E_1, \quad (3)$$

$$E_1 = \begin{pmatrix} m_k & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} m_{k-1} & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} m_1 & 1 \\ -1 & 0 \end{pmatrix},$$

где  $k$  — число форм в периоде  $ax^2 + 2bxy + cy^2$ . Следовательно, для каждого положительного целого  $n$  матрица  $E_1^n M$  обладает теми же свойствами, что и  $M$ . Мы докажем, что при достаточно большом  $n$  матрица  $E_1^n M$  имеет разложение (2).

Как и в формулировке теоремы, положим  $a = a_0$ ,  $c = a_1$  и  $b = r_0$ . Тогда формулы из предыдущего параграфа показывают, что каждый множитель матрицы  $E_1$  можно рассматривать как отображение из множества квадратичных целых вида  $a_i x + (r_i - \sqrt{D}) y$  в множество квадратичных целых вида  $a_{i+1} x + (r_{i+1} - \sqrt{D}) y$ , заданное умножением на  $r_i + \sqrt{D}$  с последующим делением на  $a_i$ . [Эта операция переводит  $a_i \cdot 1 + (r_i - \sqrt{D}) \cdot 0$  в  $r_i + \sqrt{D} = [(r_{i+1} + r_i)/a_{i+1}] a_{i+1} - (r_{i+1} - \sqrt{D})$  (где  $(r_{i+1} + r_i)/a_{i+1} = m_{i+1}$ ), а  $a_i \cdot 0 + (r_i - \sqrt{D}) \cdot 1$  переводит в  $(r_i^2 - D)/a_i = a_{i+1}$ .] Как и в гл. 7,  $r_i$  положительны, а знаки  $a_i$  чередуются. Следовательно, знаки  $m_i$  чередуются, и матрица  $E_1$  задана разложением вида (2).

Кроме того, формулы из предыдущего параграфа показывают, что матрица  $M$  соответствует отображению из множества квадратичных целых вида  $ax + (b - \sqrt{D}) y$  в множество квадратичных целых вида  $a'x + (b' - \sqrt{D}) y$ , заданному умножением на  $u + v\sqrt{D}$  с последующим делением на  $a$ . Здесь  $u + v\sqrt{D} = \alpha a + \gamma (b - \sqrt{D}) = \delta a' - \gamma (b' + \sqrt{D})$ ,  $\alpha$ ,  $\beta$ ,  $\gamma$  и  $\delta$  — элементы  $M$ . Кроме того,  $u^2 - Dv^2 = (\alpha a + \gamma b)^2 - D\gamma^2 = a^2\alpha^2 + 2ab\alpha\gamma + b^2\gamma^2 - b^2\gamma^2 + a c \gamma^2 = a [a\alpha^2 + 2b\alpha\gamma + c\gamma^2] = aa'$ . Аналогично,  $E_1$  соответствует отображению множества квадратичных целых вида  $ax + (b - \sqrt{D}) y$  в себя, заданному умножением на  $U + V\sqrt{D}$  с последующим делением на  $a$ ; здесь  $U$  и  $V$  — целые. Норма  $U + V\sqrt{D}$  равна  $U^2 - DV^2 = a^2$ . Но  $E_1$  соответствует также следующей операции: мы умножаем на  $r_0 + \sqrt{D}$  и делим на  $a_0$ , результат мы снова умножаем на  $r_1 + \sqrt{D}$  и делим на  $a_1$ , и т. д.; поэтому

$$\frac{U + V\sqrt{D}}{a} = \frac{(r_0 + \sqrt{D})(r_1 + \sqrt{D}) \dots (r_{k-1} + \sqrt{D})}{a_0 a_1 \dots a_{k-1}}.$$

В частности, поскольку  $r_i$  положительны,  $U$  и  $V$  имеют одинаковый знак.

Мы можем предположить, что  $ax^2 + 2bxy + cy^2$  — собственно примитивная форма. Тогда  $(U + V\sqrt{D})/a$  является единицей вида  $\varepsilon = g + h\sqrt{D}$ , где  $g$  и  $h$  — целые числа. Это утверждение следует из равенства

$$\begin{pmatrix} \delta' & -\gamma' \\ -\beta' & \alpha' \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix},$$

где  $\alpha', \beta', \gamma', \delta'$  — элементы  $E_1$ . Из этого равенства мы получаем, что  $\delta'a - \gamma'b = a\alpha' + b\gamma'$  и  $\delta'b - \gamma'c = a\beta' + b\delta'$ , поэтому  $a(\delta' - \alpha') = 2b\gamma'$  и  $a\beta' = -c\gamma'$ . Следовательно,  $a$  делит  $a\gamma'$ ,  $2b\gamma'$  и  $c\gamma'$ . Поскольку существуют такие целые  $k, l, m$ , что  $ka + l(2b) + mc = 1$ , мы получаем отсюда, что  $a$  делит  $\gamma'$ . Далее,  $U + V\sqrt{D} = \alpha'a + \gamma'(b - V\sqrt{D})$ , следовательно,  $a$  делит как  $U$ , так и  $V$ . Таким образом,  $(U + V\sqrt{D})/a = g + h\sqrt{D}$  и  $g + h\sqrt{D}$  должно быть единицей, поскольку его норма равна  $(U^2 - DV^2)/a^2 = 1$ .

Таким образом, матрица  $E_1$  соответствует отображению множества квадратичных целых вида  $ax + (b - V\sqrt{D})y$  в себя, заданному умножением на  $g + h\sqrt{D}$ . Следовательно, матрица  $E_1^n M$  соответствует отображению квадратичных целых вида  $ax + (b - V\sqrt{D})y$  в квадратичные целые вида  $a'x + (b' - V\sqrt{D})y$ , заданному умножением на  $(u + v\sqrt{D})(g + h\sqrt{D})^n$  с последующим делением на  $a$ . Положим  $u' + v'\sqrt{D} = (u + v\sqrt{D})(g + h\sqrt{D})^n$ . Тогда, как и в гл. 7, можно показать, что при большом  $n$  знаки  $u'$  и  $v'$  совпадают и абсолютная величина  $v'$  велика. Далее, снова как в гл. 7, мы можем доказать, что соответствующая  $2 \times 2$ -матрица  $E_1^n M$  обладает свойствами  $|X| \geq |Z| \geq |W|$ ,  $|X| \geq |Y| \geq |W|$  и имеет разложение вида (2). Следовательно, не ограничивая общности, можно считать, что сама матрица  $M$  имеет такой вид.

Умножение на  $g + h\sqrt{D}$  отображает квадратичные целые вида  $a'x + (b' - V\sqrt{D})y$  в себя (квадратичное целое  $w + z\sqrt{D}$  имеет такой вид тогда и только тогда, когда  $w + zb' \equiv 0 \pmod{a'}$ ; поскольку  $D \equiv b'^2 \pmod{a'}$ , то последнее условие выполняется для  $(g + h\sqrt{D})(w + z\sqrt{D})$ , если оно справедливо для  $w + z\sqrt{D}$ ). Следовательно, это умножение соответствует  $2 \times 2$ -матрице  $E_2$ , для которой  $E_1 M = M E_2$ . Матрица  $E_2$  имеет разложение вида (2), и знаки всех разложений согласуются таким образом, что  $E_1 M$  и  $M E_2$  являются разложениями вида (2). Тогда равенства  $E_1^n M = M E_2^n$ , справедливые при всех  $n > 0$ , и единственность разложений вида (2) показывают, что множители матрицы  $M$  вырезаются из разложения  $E_1^n$  при большом  $n$ . Поэтому из разложения (2) следует, что матрица  $\pm M$  задает то самое преобразование, которое мы получаем, применяя циклический метод к  $ax^2 + 2bxy + cy^2$ . Следовательно,  $a'x^2 + 2b'xy + c'y^2$  принадлежит периоду  $ax^2 + 2bxy + cy^2$ , что и требовалось доказать.

## Упражнения

1. Докажите, что число собственно примитивных классов собственной эквивалентности форм с данным детерминантом конечно. Получите отсюда, что во всех случаях группа классов дивизоров конечна.

2. Пусть  $ax^2 + 2bxy + cy^2$  — приведенная форма и  $D = b^2 - ac > 0$ . Предположим, что единица  $\varepsilon = g + h\sqrt{D}$  найдена так же, как и в доказательстве теоремы. Докажите, что норма  $\varepsilon$  равна 1 и что все единицы порядка  $\{x + y\sqrt{D}\}$ , имеющие единичную норму, совпадают с  $\pm\varepsilon^n$ . Покажите, что единица с нормой  $-1$  существует только тогда, когда каждая форма  $ax^2 + 2bxy + cy^2$  несобственно эквивалентна своему отрицанию  $-ax^2 - 2bxy - cy^2$ , а потому собственно эквивалентна  $-ax^2 + 2bxy - cy^2$ . Если эти условия выполнены, приведите алгоритм нахождения единицы с нормой  $-1$  и покажите, что квадрат этой единицы равен определенной выше единице  $\varepsilon$ . Подведите итоги этим результатам, разработав для любого порядка  $\{x + y\sqrt{D}\}$  процедуру нахождения *основной единицы*, т. е. такой единицы  $\varepsilon$ , что формула  $\pm\varepsilon^n$  дает каждую единицу, и притом только один раз.

3. Найдите приведенную форму, собственно эквивалентную форме  $x^2 - 67y^2$ ; используйте упр. 2 для нахождения общего решения уравнения Пелля  $u^2 = 67v^2 + 1$ .

4. Найдите приведенную форму, собственно эквивалентную форме  $x^2 + xy - 15y^2$ , и используйте упр. 2 для нахождения основной единицы порядка  $\{x + y\sqrt{61} : x, y \text{ — целые или полуцелые}\}$ .

5. Найдите группу классов дивизоров, соответствующую порядку  $\{x + y\sqrt{99} : x, y \text{ — целые}\}$ . [ $-1$  и  $2$  разветвляются,  $5$  распадается,  $s = 3$ . Дивизоры  $I$ ,  $(-1, *)$ ,  $(2, *)$  и  $(-1, *) (2, *)$  не эквивалентны. Критерий проверки, является ли дивизор  $(5, 1)$  главным, показывает не только то, что  $(5, 1)$  — не главный дивизор, но и что он не эквивалентен ни одному из 4 дивизоров, приведенных выше, и, кроме того,  $(5, 1) \sim (-1, *) (2, *) (5, 1)$ . Поэтому формула  $(-1, *)^i (5, 1)^j$  при  $i = 0, 1; j = 0, 1, 2, 3$  дает 8 неэквивалентных дивизоров. Они соответствуют 8 периодам приведенных форм. Покажите, что каждая приведенная форма лежит в одном из этих периодов.]

6. Найдите группу классов дивизоров, соответствующую порядку  $\{x + y\sqrt{-99} : x, y \text{ — целые}\}$ .

7. Докажите, что если  $\alpha$  и  $\gamma$  — заданные взаимно простые целые, то существуют такие целые  $\beta$  и  $\delta$ , что

$$\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1.$$

Получите отсюда, что если форма  $ax^2 + 2bxy + cy^2$  *собственно* представляет  $m$  (со взаимно простыми  $x$  и  $y$ ), то она *собственно* эквивалентна форме, первый коэффициент которой равен  $m$ . Используя этот факт, докажите, что метод из § 8.2 дает представление формой  $ax^2 + 2bxy + cy^2$  всегда, когда такое представление возможно.

8. Опишите в деталях (если возможно, напишите программу для ЭВМ) процедуру нахождения всех решений уравнения вида  $ax^2 + 2bxy + cy^2 = m$ , где  $a, b, c$  и  $m$  — целые, заключенные в некоторых заранее фиксированных границах.

9. Докажите, что  $3 \not\equiv x^2 - 37y^2$ ,  $151 = x^2 - 37y^2$ , несмотря на то что  $3 \equiv 151 \pmod{4 \cdot 37}$ . Это дает контрпример к гипотезе Эйлера из упр. 8 к § 7.9 с меньшим детерминантом  $D$ , чем в контрпримере Лагранжа.

## 8.5. Примеры

Как было показано в § 7.6, число классов при <sup>1)</sup>  $D = -163$  равно 1. Если в этой ситуации мы рассмотрим порядок индекса 2, совпадающий с  $\{x + y\sqrt{-163} : x, y \text{ — целые}\}$ , то его число клас-

<sup>1)</sup> В обозначениях из предыдущего параграфа здесь  $D = -163/4$ .

сов будет больше 1. Действительно, если мы разрешаем знаменателям содержать 2, то  $(41, 1)$  является дивизором целого  $(1 - \sqrt{-163})/2$ . Однако этот дивизор перестает быть главным в рассматриваемом порядке индекса 2, поскольку он соответствует бинарной квадратичной форме  $41x^2 + 2xy + 4y^2$ , и циклический метод

$$\begin{array}{cccc} 1 & -1 & 1 & \dots \\ 41 & 4 & 41 & \dots \end{array}$$

показывает, что эта форма не эквивалентна в собственном смысле форме  $x^2 + 163y^2$ , соответствующей дивизору  $I$ .

[По-видимому, здесь наступил самый подходящий момент для того, чтобы остановиться и обсудить любопытную этимологию прилагательного «главный» в словосочетаниях «главный дивизор» или «главный идеал». Простейшая бинарная квадратичная форма с детерминантом  $D$  равна  $x^2 - Dy^2$ . Поэтому достаточно естественно, что Гаусс назвал эту форму *главной формой* с детерминантом  $D$ . Ее класс собственной эквивалентности — класс главной формы — он назвал *главным классом*. При соответствии из § 8.3 этот класс отвечает классу дивизора  $I$ . Поэтому такой класс дивизоров, который является единичным элементом группы классов дивизоров, естественно называется *главным классом*. Тогда дивизор принадлежит главному классу в том и только в том случае, когда он является дивизором некоторого (неидеального) элемента, а идеал принадлежит главному классу тогда и только тогда, когда он совпадает с множеством всех элементов, делящихся на некоторый (неидеальный) элемент. Таким образом, идеал кольца называется *главным*, если он совпадает с множеством всех элементов, делящихся на некоторый данный элемент кольца.]

Пусть  $A = (41, 1)$ . Тогда  $A^2$  — дивизор с нормой  $41^2 = 1681$  и  $A^2$  делит  $(1 - \sqrt{-163})^2 = -162 - 2\sqrt{-163} = -2(81 + \sqrt{-163})$ , поэтому  $\sqrt{-163} \equiv -81 \pmod{A^2}$ . Следовательно, применение циклического метода к  $A^2$  дает

$$\begin{array}{cccc} -81 & 1 & -1 & 1 \dots \\ 4 & 41 & 4 & \dots \end{array}$$

Таким образом,  $A^2 \sim \bar{A}$ ; значит,  $A^3 \sim I$ . Докажем, что эти три класса дивизоров  $I$ ,  $A$  и  $A^2$  исчерпывают все классы из группы классов дивизоров. Любой дивизор, взаимно простой с 2, соответствует форме  $ax^2 + 2bxy + cy^2$ , где  $a, b, c$  — целые числа,  $a > 0$ ,  $c > 0$  и  $b^2 - ac = -163$ . При помощи циклического метода такую форму можно привести к форме, коэффициенты которой удовлетворяют неравенствам  $a \leq c$ ,  $|b| \leq a/2$ . Тогда  $a^2 \leq ac = b^2 + 163 \leq \frac{1}{4}a^2 + 163$ ,  $a^2 \leq (4 \cdot 163)/3$ ,  $a \leq 14$ ,  $|b| \leq 7$ . Поэтому

мы должны найти малые делители числа  $b^2 + 163$  при  $b = 0, 1, \dots, 7$ . Кроме  $a = 1, b = 0$  единственными малыми делителями этого числа являются  $a = 2$  или  $4$ . Доказать это утверждение можно следующим образом. Заметим, что при  $p = 3, 5, 7$  и  $11$  детерминант  $D = -163$  не является квадратом по модулю  $p$ , поэтому  $p \mid a$  влечет за собой  $a \nmid b^2 + 163$ . Следовательно,  $a$  может делиться только на простое число  $2$  и  $8 \nmid a$ , поскольку  $b^2 + 163 \equiv b^2 + 3 \not\equiv 0 \pmod{8}$ . Если  $a = 2$ , то  $b = \pm 1, c = 82$  и форма  $ax^2 + 2bxy + cy^2$  не является собственно примитивной. Это оставляет нам только три возможности:  $a = 1, b = 0$  и  $a = 4, b = \pm 1$ . Следовательно, имеется только три класса, что и требовалось доказать. Таким образом, число классов порядка  $\{x + y\sqrt{-163} : x, y \text{ — целые}\}$  равно <sup>1)</sup> 3 и дивизоры  $A, A^2$  и  $A^3 \sim I$  образуют систему представителей.

Гаусс (Disquisitiones Arithmeticae, Arts. 223, 224 и 226) рассмотрел порядок  $\{x + y\sqrt{-235} : x, y \text{ — целые}\}$ . В этом случае каждая форма эквивалентна форме  $ax^2 + 2bxy + cy^2$ , где  $c \geq a > 0, |b| \leq a/2$ . Из этих неравенств следует, что  $a^2 \leq 4 \cdot 235/3, a \leq 17$ . Любой простой делитель числа  $a$  должен обладать тем свойством, что по модулю этого делителя  $-235$  является квадратом. Ясно, что таким свойством обладают  $2$  и  $5$ , но не обладают  $3, 7, 11, 17$ . Кроме того,  $-235 \equiv -1 \equiv 5^2 \pmod{13}$ , и к числам  $2$  и  $5$  следует добавить  $13$ . Пусть  $A = (13, 5)$ . Этот дивизор не является главным, поскольку

$$\begin{array}{ccccc} 5 & & -5 & & 5 \dots \\ 13 & 20 & & & 13 \dots \end{array}$$

Норма его квадрата равна  $N(A^2) = 169$ . Дивизор  $A^2$  делит  $(5 - \sqrt{-235})^2 = -210 - 10\sqrt{-235}$ , поэтому  $\sqrt{-235} \equiv -21 \pmod{A^2}$ . Следовательно, вычисления, производимые с целью установить, является ли  $A^2$  главным дивизором, а именно

$$\begin{array}{ccccc} -21 & 1 & & -1 \dots \\ 169 & 4 & 59 & \dots \end{array}$$

показывают, что  $A^2$  — неглавный дивизор, но он эквивалентен дивизору  $(59, -1)$ . Таким образом,  $A^3 \sim A(59, -1)$ . Норма последнего дивизора равна  $13 \cdot 59 = 767$ , и этот дивизор делит  $(5 - \sqrt{-235})(1 + \sqrt{-235}) = 240 + 4\sqrt{-235}$ . Поэтому циклический метод

$$\begin{array}{ccccc} -60 & 0 & 0 & & \\ 767 & 5 & 47 & 5 \dots \end{array}$$

<sup>1)</sup> В немецком издании [G2] Disquisitiones Arithmeticae на стр. 351 ошибочно указана классификация II.3 (а не I.3).



показывает, что  $A^3 \sim (5, *)$ . Поскольку  $(5, *)^2$  является дивизором числа 5, то  $A^6 \sim I$ , но, как мы доказали выше,  $A^2 \not\sim I$  и  $A^3 \not\sim I$ . Следовательно, 6 дивизоров  $A, A^2, A^3, A^4, A^5, A^6 \sim I$  принадлежат различным классам. Эти шесть классов образуют всю группу классов дивизоров. Действительно, они содержат приведенные формы с коэффициентами  $a = 1, b = 0; a = 4, b = \pm 1; a = 5, b = 0$  и  $a = 13, b = \pm 5$ . Другими возможными значениями  $a \leq 17$  являются  $a = 2$  или  $a = 10$ , но они не приводят к собственно примитивным формам.

Рассмотрим теперь порядок  $\{x + y\sqrt{60}: x, y \text{ — целые}\} = \{x + 2y\sqrt{15}: x, y \text{ — целые}\}$ . Здесь  $D > 0$ , поэтому мы должны рассмотреть дивизор  $(-1, *)$ . Вычисления

$$\begin{array}{cccccc} 7 & 4 & 4 & 7 & 7 & \dots \\ -1 & 11 & -4 & 11 & -1 & \dots \end{array}$$

показывают, что  $(-1, *)$  не является главным дивизором. При  $D = 15$  простое 3 разветвляется. Поскольку 3 взаимно просто с 2, дивизор  $(3, *)$  принадлежит некоторому классу рассматриваемой группы классов дивизоров. Этот класс не является главным:

$$\begin{array}{cccccc} 6 & 2 & 5 & 5 & 2 & 6 & 6 & \dots \\ 3 & -8 & 7 & -5 & 7 & -8 & 3 & \dots \end{array}$$

и эти же вычисления показывают не только то, что дивизор  $(-1, *)(3, *)$  с нормой  $-3$  не главный, но и то, что четыре дивизора  $I, (-1, *), (3, *)$  и  $(-1, *) (3, *)$  принадлежат различным классам, поскольку они приводят к разным периодам форм. Квадрат любого из этих классов равен классу  $I$ , поэтому легко найти произведение любой пары из этих классов. Для того чтобы доказать, что это дает нам полное описание группы классов дивизоров, достаточно доказать, что эти четыре класса содержат все дивизоры. Каждая форма собственно эквивалентна форме  $ax^2 + 2bxy + cy^2$ , для которой  $a \leq 2\sqrt{60/3} < 10$ . Кроме того,  $b^2 \equiv 60 \pmod{a}$ ,  $b^2 < 60$  и  $(b + |a|)^2 > 60$ . В рассмотренных выше классах содержатся формы, для которых  $a = \pm 1, \pm 3, \pm 4, \pm 5, \pm 7, \pm 8$ . При  $a = \pm 1$ ,  $a = \pm 3$ ,  $a = \pm 5$  возможно только одно значение  $b$ . Если  $a = 4$ , то  $b^2 \equiv 0 \pmod{4}$ ,  $b \equiv 0$  или  $2 \pmod{4}$ , и случай  $b \equiv 2 \pmod{4}$ ,  $b = 6$  не включается в рассмотренные выше. Но тогда  $c = (b^2 - D)/a = -6$ , и эта форма не является собственно примитивной. Аналогично,  $a = -4$ ,  $b = 6$  приводит к не собственно примитивной форме. Если  $a = \pm 7$ , то возможны только два значения  $b$ ,  $b \equiv 2$  или  $5 \pmod{a}$ . Эти возможности содержатся в рассмотренных выше случаях. Если  $a = \pm 8$ , то сравнение  $b^2 \equiv 4 \pmod{8}$  имеет два решения  $b \equiv 2$  или  $6 \pmod{8}$  и соответствующие формы принадлежат введенным выше четырём классам. Пусть теперь  $a = \pm 2$ ;

тогда  $b = 6$  и  $c = \mp 12$ , т. е. форма не является собственно примитивной. Наконец, если  $a = \pm 6$ , то  $b^2 \equiv 0 \pmod{6}$ ,  $b \equiv \equiv 0 \pmod{6}$ ,  $b = 6$ ,  $c = \mp 4$  и соответствующая форма снова не является собственно примитивной. Следовательно, группа классов дивизоров совпадает с описанной выше группой из четырех элементов.

Наконец, рассмотрим еще один случай, разобранный Гауссом (Disquisitiones Arithmeticae, Art. 226): группу классов дивизоров порядка  $\{x + y\sqrt{45}: x, y \text{ — целые}\}$ . Индекс  $s$  этого порядка равен 6, поскольку  $45 = 3^2 \cdot 5$  и  $5 \equiv 1 \pmod{4}$ . В этом случае дивизор  $(-1, *)$  не является главным. Однако циклический метод показывает, что  $(5, *) \sim (-1, *)$ , следовательно,  $(-1, *) (5, *) \sim I$ . Применяя процесс исключения, аналогичный использованному выше, мы получим, что группа классов дивизоров содержит в точности два элемента: классы дивизоров  $I$  и  $(-1, *)$ . (Значения  $a = \pm 2, \pm 3$  приводят к не собственно примитивным формам; 45 не является квадратом по модулю 7, поэтому  $a$  не может быть равно  $\pm 7$ ;  $a = \pm 5, \pm 6$  приводят к уже рассмотренным формам. Если  $a = \pm 4$ , то  $b = 3$  или  $b = 5$  и соответствующие формы отвечают уже найденным выше периодам.)

## Упражнения

Найдите группу классов дивизоров (т. е. систему представителей и таблицу умножения) следующих порядков.

1.  $\{x + y\sqrt{-99}: x, y \text{ — целые}\}$ . (Disquisitiones Arithmeticae, Art. 226. Циклическая группа шестого порядка.)

2.  $\{x + y\sqrt{-117}: x, y \text{ — целые}\}$ . (Число классов равно 8.)

3.  $\{x + y\sqrt{-531}: x, y \text{ — целые}\}$ . (Disquisitiones Arithmeticae, Art. 255. Число классов равно 18.)

4.  $\{x + y\sqrt{305}: x, y \text{ — целые}\}$ . (Число классов равно 4.)

5.  $\{x + y\sqrt{305}: x, y \text{ — целые или полуцелые}\}$ .

6.  $\{x + y\sqrt{-59}: x, y \text{ — целые}\}$ . (Ср. с упр. 3.)

7.  $\{x + y\sqrt{-59}: x, y \text{ — целые или полуцелые}\}$ .

8.  $\{x + y\sqrt{-531}: x, y \text{ — целые или полуцелые}\}$ .

9. Просмотрите любую из таблиц бинарных квадратичных форм, помещенных в указанных ниже источниках, и проверьте ее для различных значений  $D$ .

Cayley A., Tables des formes quadratiques binaires pour les déterminants négatifs depuis  $D = -1$  jusqu'à  $D = -100$ , pour les déterminants positifs non carrés depuis  $D = 2$  jusqu'à  $D = 99$  et pour les treize déterminants négatifs irréguliers qui se trouvent dans le premier millier, *Jour. für Math.* (Crelle), B. LX (1862), 357—372. [См. также Cayley A., Mathematical Papers, vol. 5, pp. 141—156.]

Ince E. L., Cycles of Reduced Ideals in Quadratic Fields, British Assn. for the Advancement of Science, Mathematical Tables, Vol. IV, Cambridge University Press, 1966.

10. Проверьте различные элементы табл. III из книги Cohn H., A Second Course in Number Theory, Wiley, New York, 1962.

11. Докажите следующую лемму (мы использовали ее в § 3.3 без доказательства): если  $a$  и  $b$  взаимно просты, то каждый нечетный делитель числа  $a^2 - 5b^2$  можно записать в виде  $p^2 - 5q^2$ .

12. В теории Гаусса группы классов дивизоров можно следующим образом разделить на *роды*. Такая группа соответствует некоторому порядку вида  $\{x + y \sqrt{D} : x, y \text{ — целые}\}$ . Для каждого нечетного простого делителя детерминанта  $D$  определим *характер* соответствующей группы в точности так же, как в § 7.9. Если  $D \equiv 1 \pmod{4}$ , то эти характеры образуют весь характер. Если  $D \equiv 2$  или  $3 \pmod{4}$ , то полный характер содержит дополнительный знак, определенный табл. 7.9.1. При  $D \equiv 0 \pmod{4}$  следует различать два случая. Если  $D \equiv 4 \pmod{8}$ , то нечетные числа вида  $x^2 - Dy^2$  сравнимы с 1 или 5 по модулю 8, т. е. все они сравнимы с 1 по модулю 4, и дополнительный знак есть «+», если  $n \equiv 1 \pmod{4}$ , и «—», если  $n \equiv 3 \pmod{4}$  (как и при  $D \equiv 3 \pmod{4}$ ). Если  $D \equiv 0 \pmod{8}$ , то нечетные числа вида  $x^2 - Dy^2$  сравнимы с 1 по модулю 8 и характер имеет *два* дополнительных знака, в качестве которых можно взять знаки  $\binom{-1}{n}$  и  $\binom{2}{n}$ . В каждом из приведенных выше примеров из основного текста и упражнений (за исключением упр. 5, 7 и 8) и в случае порядков  $\{x + y \sqrt{D} : x, y \text{ — целые}\}$  при  $D = 24, 8, -8, -16, -24$  найдите разбиение группы классов дивизоров на роды и определите все встречающиеся характеры. (Например, при  $D = 60$  группа классов дивизоров состоит из 4 родов, каждый из которых содержит один класс — классификация IV.1 в обозначениях из § 7.9, и в действительности встречаются характеры  $+++$ ,  $+-$ ,  $-+$  и  $---$ .) Обратите внимание на то, что во всех случаях в действительности встречается ровно половина всех возможных характеров (как и в § 7.11). Гаусс доказал, что так должно быть всегда (Disquisitiones Arithmeticae, Arts. 257—261).

## 8.6. Гауссова композиция форм

Вычисления из предыдущего параграфа показывают, что в процессе применения циклического метода для нахождения элементов группы классов дивизоров проще всего рассматривать эти классы не как классы эквивалентности дивизоров, а как классы собственной эквивалентности бинарных квадратичных форм. Поэтому может показаться естественным не прибегать вообще к понятию классов дивизоров, а, следуя Гауссу, формулировать всю теорию на языке бинарных квадратичных форм. Правда, против этого есть возражение Куммера, что понятие собственной эквивалентности становится естественнее, если рассматривать его с точки зрения теории дивизоров. Однако одного этого соображения едва ли достаточно для того, чтобы оправдать все построения теории дивизоров.

Преимущество теории дивизоров состоит в том, что она дает объяснение операции *умножения* классов. С точки зрения классов дивизоров вряд ли можно найти более естественное умножение: произведение класса дивизора  $A$  на класс дивизора  $B$  равно классу  $AB$ . В то же время описать это умножение с точки зрения классов собственной эквивалентности форм чрезвычайно трудно. В этом параграфе мы ограничимся лишь кратким перечислением

множества шагов, необходимых для определения этой операции. Гаусс назвал ее *композицией форм*.

Тот факт, что Куммер не говорит об этом преимуществе своего подхода, а ограничивается лишь замечанием, что его теория «в значительной степени аналогична очень трудному разделу *De compositione formarum* из книги Гаусса» [К7, стр. 325], ясно показывает, что Куммер не разработал детально «теорию комплексных чисел вида  $x + y\sqrt{D}$ », о которой он говорит в предыдущем абзаце. Другое свидетельство тесной связи между теорией дивизоров квадратичных целых и композицией форм содержится в письме Куммера Кронекеру от 14 июня 1846 г. [К5, стр. 68]. Здесь Куммер пишет: «[Дирихле] показал мне, основываясь на письменных и устных замечаниях Гаусса, что Гаусс в период завершения раздела о композиции форм в *Disquisitiones Arithmeticae* уже использовал нечто похожее на идеальные делители, но он так и не смог найти для них прочную основу; в частности, в заметке о разложении многочленов на линейные множители Гаусс говорит: «Если бы я захотел продолжать пользоваться мнимыми величинами таким же образом, как это делали математики предшествующих поколений, то одно очень трудное из моих ранних исследований можно было бы выполнить очень просто». Позже Гаусс сказал Дирихле, что здесь он имел в виду композицию форм».

Изобретение *композиции форм* было большим вкладом Гаусса в теорию бинарных квадратичных форм. (Применение циклического метода для решения уравнений  $ax^2 + 2bxy + cy^2 = m$  было хорошо известно Лагранжу и Эйлеру, и Гаусс изложил его в своих *Disquisitiones Arithmeticae* главным образом как резюме сделанного его предшественниками.) Частный случай композиции форм, который был известен задолго до Гаусса, содержится в формуле

$$(x^2 + ny^2)(u^2 + nv^2) = (xu - nuy)^2 + n(xv + yu)^2, \quad (1)$$

показывающей, что произведение двух чисел вида  $x^2 + ny^2$  снова имеет тот же самый вид. Другим примером является формула

$$(2x^2 + 2xy + 3y^2)(2u^2 + 2uv + 3v^2) = X^2 + 5Y^2, \quad (2)$$

где

$$X = 2xu + xv + yu - 2yv,$$

$$Y = xv + yu + yv.$$

Эту формулу можно использовать для доказательства гипотезы Ферма о числах вида  $x^2 + 5y^2$  (см. упр. 1).

Вообще, бинарная квадратичная форма  $\alpha x^2 + 2\beta xy + \gamma y^2$  называется *композицией* двух других форм  $ax^2 + 2bxy + cy^2$  и  $a'x^2 + 2b'xy + c'y^2$ , если существует равенство вида

$$(ax^2 + 2bxy + cy^2)(a'u^2 + 2b'uv + c'v^2) = \alpha X^2 + 2\beta XY + \gamma Y^2,$$

где  $X$  и  $Y$  — билинейные функции от  $(x, y)$  и  $(u, v)$ , т. е.

$$X = rxi + r'xv + r''yu + r'''yv,$$

$$Y = qxi + q'xv + q''yu + q'''yv$$

с данными целыми  $r, r', r'', r''', q, q', q'', q'''$ , и где шесть определителей

$$P = \begin{vmatrix} r & r' \\ q & q' \end{vmatrix}, \quad Q = \begin{vmatrix} r & r'' \\ q & q'' \end{vmatrix}, \quad R = \begin{vmatrix} r & r''' \\ q & q''' \end{vmatrix},$$

$$S = \begin{vmatrix} r' & r'' \\ q' & q'' \end{vmatrix}, \quad T = \begin{vmatrix} r' & r''' \\ q' & q''' \end{vmatrix}, \quad U = \begin{vmatrix} r'' & r''' \\ q'' & q''' \end{vmatrix}$$

не имеют общих делителей, больших 1. Последнее условие относительно  $P, Q, R, S, T, U$  является условием типа невырожденности. Гаусс не дает для него никакой мотивировки (как, впрочем, и для других аспектов этой теории).

Путем мощных алгебраических выкладок Гаусс показывает, что в любой композиции форм тройка целых чисел  $(P, R - S, U)$  пропорциональна  $(a, 2b, c)$ , а  $(Q, R + S, T)$  пропорциональна  $(a', 2b', c')$ . Например, в композиции (1) наборы  $r$  и  $q$  равны

$$\begin{array}{cccc} 1 & 0 & 0 & -n \\ 0 & 1 & 1 & 0 \end{array}$$

поэтому  $P = 1, Q = 1, R = 0, S = 0, T = n, U = n, (P, R - S, U) = (1, 0, n)$  и  $(Q, R + S, T) = (1, 0, n)$ . Аналогично, в композиции (2) наборы  $r$  и  $q$  равны

$$\begin{array}{cccc} 2 & 1 & 1 & -2 \\ 0 & 1 & 1 & 1 \end{array}$$

следовательно,  $P = 2, Q = 2, R = 2, S = 0, T = 3, U = 3, (P, R - S, U) = (2, 2, 3)$  и  $(Q, R + S, T) = (2, 2, 3)$ . Если первый из этих коэффициентов пропорциональности положителен, то Гаусс говорит, что форма  $a'x^2 + 2b'xy + c'y^2$  входит в эту композицию *прямо*, а если этот коэффициент пропорциональности отрицателен, то форма входит в композицию *обратно*. Аналогично, форма  $ax^2 + 2bxy + cy^2$  входит в композицию *прямо* или *обратно*, если коэффициент пропорциональности между  $(Q, R + S, T)$  и  $(a', 2b', c')$  соответственно положителен или отрицателен. Таким образом, в приведенные выше композиции обе формы входят *прямо*. В то же время в композиции

$$(x^2 + ny^2)(u^2 + nv^2) = (xu + nyv)^2 + n(xv - yu)^2$$

наборы  $r$  и  $q$  равны

$$\begin{array}{cccc} 1 & 0 & 0 & n \\ 0 & 1 & -1 & 0 \end{array}$$

следовательно,  $P = 1$ ,  $Q = -1$ ,  $R = 0$ ,  $S = 0$ ,  $T = -n$ ,  $U = n$ ,  $(P, R - S, U) = (1, 0, n)$ ,  $(Q, R + S, T) = (-1, 0, -n)$ , и первая форма входит в композицию *обратно*, а вторая — *прямо*.

В дальнейшем мы будем рассматривать только такие композиции, в которые оба сомножителя входят *прямо*. Основные результаты Гаусса о композиции форм кратко можно сформулировать следующим образом. Гаусс доказал <sup>1)</sup>, что операция композиции корректно определена на множестве классов *собственной* эквивалентности бинарных квадратичных форм данного детерминанта (по этой причине различие собственной и несобственной эквивалентности необходимо для теории Гаусса) и что она определяет на множестве классов собственно примитивных форм структуру коммутативной *группы*. Подробнее, среди прочих результатов Гаусс доказал следующее.

(1) Предположим, что  $F$  можно записать в виде композиции  $f$  и  $f'$ , а  $F'$  — в виде композиции  $f$  и  $f''$ . Если  $f'$  и  $f''$  собственно эквивалентны, то  $F$  и  $F'$  собственно эквивалентны.

(2) Если  $F$  можно записать в виде композиции  $f$  и  $f'$ , то  $F$  можно записать в виде композиции  $f'$  и  $f$ . (Это просто.)

(3) Композиция, рассматриваемая с точностью до собственной эквивалентности, *ассоциативна*. Точнее, предположим, что  $F$  — композиция  $f$  и  $f'$ ,  $\mathcal{F}$  — композиция  $F$  и  $f''$ ,  $F'$  — композиция  $f'$  и  $f''$  и  $\mathcal{F}'$  — композиция  $f$  и  $F'$ ; тогда  $\mathcal{F}$  и  $\mathcal{F}'$  собственно эквивалентны. (Это необычайно трудно. См. Disquisitiones Arithmeticae, Art. 240.)

(4) Если заданы две формы  $f$  и  $f'$  с одним и тем же детерминантом, то можно найти третью форму  $F$ , которая имеет тот же детерминант и является композицией  $f$  и  $f'$ . (Это далеко не очевидно.)

(5) Если заданы две собственно примитивные формы  $f$  и  $f'$ , то найдется такая собственно примитивная форма  $f''$ , что композиция  $f$  и  $f''$  собственно эквивалентна  $f'$ . (См. Art. 251.)

Обратите внимание, что Гаусс повелительным жестом определяет композицию для *любых* двух форм, хотя при фактическом вычислении *класса* композиции ради удобства можно заменять формы на собственно эквивалентные (согласно (1)). Это можно следующим образом использовать при вычислении композиции двух собственно примитивных форм  $ax^2 + 2bxy + cy^2$  и  $a'x^2 + 2b'xy + c'y^2$  с одним и тем же детерминантом  $b^2 - ac = b'^2 - a'c'$ .

Согласно § 8.3, можно предположить (не ограничивая общности), что  $a$  нечетно и взаимно просто с  $D = b^2 - ac$ . Аналогично, можно считать, что  $a'$  нечетно и взаимно просто с  $D$  и  $a$ . Замена переменных  $x' = x + ny$ ,  $y' = y$  дает нам новую форму, соб-

<sup>1)</sup> Гаусс сделал даже больше того, что здесь описано, поскольку он рассматривал композицию форм разных детерминантов.



ственно эквивалентную исходной. В этой форме  $a$  остается прежним, а  $b$  заменяется на  $b + na$ . Следовательно,  $b$  можно заменить на любое число, сравнимое с  $b$  по модулю  $a$ . Аналогично,  $b'$  можно заменить на любое число, сравнимое с  $b'$  по модулю  $a'$ . Согласно китайской теореме об остатках, существует такое целое  $B$ , что  $B \equiv b \pmod{a}$  и  $B \equiv b' \pmod{a'}$ ; поэтому, не ограничивая общности, можно предположить, что формы, композицию которых мы составляем, имеют вид  $ax^2 + 2Bxy + cy^2$  и  $a'x^2 + 2Bxy + c'y^2$ , где  $a$  и  $a'$  — нечетные целые, взаимно простые друг с другом и с  $D$ . Но  $B^2 - D = ac = a'c'$  и  $a, a'$  взаимно просты; следовательно,  $B^2 - D = aa'e$  для некоторого целого  $e$  и рассматриваемые формы имеют вид  $ax^2 + 2Bxy + a'ey^2$  и  $a'x^2 + 2Bxy + aey^2$ .

Короче говоря, без ограничения общности можно считать, что  $a$  и  $a'$  — нечетные целые, взаимно простые друг с другом и с  $D$ , и что  $b = b'$ ; в этом случае  $c = a'e$  и  $c' = ae$  при некотором целом  $e$ . Поэтому задача сводится к нахождению композиции двух таких форм. После трудных вычислений (*Disquisitiones Arithmeticae*, Art. 243) Гаусс объявляет, что в этом случае форма  $aa'x^2 + 2bxy + ey^2$  является композицией  $ax^2 + 2bxy + a'ey^2$  и  $a'x^2 + 2bxy + aey^2$ . Это утверждение можно проверить непосредственно, воспользовавшись уравнением

$$(ax^2 + 2bxy + a'ey^2)(a'u^2 + 2buv + aev^2) = aa'X^2 + 2bXY + eY^2, \quad (3)$$

из которого мы должны найти  $X$  и  $Y$ . Поскольку  $aa'e = b^2 - D$ , первый множитель в левой части можно записать в виде

$$\frac{1}{a} [(ax + by)^2 - (b^2 - b^2 + D)y^2] = \frac{1}{a} N[(ax + by) - y\sqrt{D}].$$

Остальные две формы также можно переписать аналогичным образом, и, умножив обе части уравнения (3) на  $aa'$ , мы приведем его к виду

$$N[(ax + by) - y\sqrt{D}] N[(a'u + bv) - v\sqrt{D}] = N[aa'X + bY - Y\sqrt{D}].$$

Поскольку норма произведения равна произведению норм, это наводит нас на мысль о том, что

$$\begin{aligned} aa'X + bY - Y\sqrt{D} &= (ax + by - y\sqrt{D})(a'u + bv - v\sqrt{D}) = \\ &= -\sqrt{D}[axv + byv + a'yu + byv] + aa'xu + abxv + \\ &\quad + a'byu + b^2yv + Dyv, \end{aligned}$$

$$Y = axv + byv + a'yu + byv,$$

$$\begin{aligned} aa'X &= aa'xu + abxv + a'byu + b^2yv + Dyv - bY = \\ &= aa'xu + 0 \cdot xv + 0 \cdot yu - b^2yv + Dyv, \end{aligned}$$

$$X = xu - eyv.$$

(Гаусс, конечно, не одобрил бы использование  $\sqrt{D}$  в этих вычислениях.) Эти вычисления можно обратить, и при *определенных* таким образом  $X$  и  $Y$  выполняется равенство (3); при этом наборы  $p$  и  $q$  равны

$$\begin{pmatrix} 1 & 0 & 0 & -e \\ 0 & a & a' & 2b \end{pmatrix}$$

Следовательно,  $P = a$ ,  $Q = a'$ ,  $R = 2b$ ,  $S = 0$ ,  $T = ea$ ,  $U = ea'$ . Таким образом, равенство (3) описывает композицию (при взаимно простых  $a$  и  $a'$ ), в которую обе формы входят прямо.

Утверждение о том, что гауссова композиция совпадает с естественной композицией дивизоров, можно доказать следующим образом. В этом случае снова достаточно ограничиться нечетными  $a$  и  $a'$ , взаимно простыми друг с другом и с  $D$ , и  $b = b'$ . Тогда в теореме из § 8.3 форма  $ax^2 + 2bxy + cy^2$  соответствует дивизору  $A$ , который удовлетворяет условиям  $N(A) = a$ ,  $b \equiv \sqrt{D} \pmod{A}$ . Аналогично,  $a'x^2 + 2bxy + c'y^2$  соответствует  $A'$  с  $N(A') = a'$  и  $b \equiv \sqrt{D} \pmod{A'}$ . Тогда  $N(AA') = aa'$  и  $b \equiv \sqrt{D} \pmod{AA'}$  (поскольку дивизор  $b - \sqrt{D}$  делится на единственный дивизор с нормой  $a$  и на единственный дивизор с нормой  $a'$ , а целые  $a$  и  $a'$  взаимно просты). Этот дивизор соответствует форме  $aa'x^2 + 2bxy + ey^2$ , где  $e = (b^2 - D)/aa'$ , что и требовалось показать.

## Упражнения

1. Используйте формулу (2) для доказательства гипотезы Ферма, согласно которой произведение двух простых  $p_1, p_2 \equiv 3$  или  $7 \pmod{20}$  имеет вид  $p_1p_2 = x^2 + 5y^2$ . [Докажите, что при  $p \equiv 3$  или  $7 \pmod{20}$  существует бинарная квадратичная форма  $px^2 + 2dxy + ey^2$  с детерминантом  $-5$ . Эта форма эквивалентна либо  $x^2 + 5y^2$ , либо  $2x^2 + 2xy + 3y^2$ . Так как  $p$  не представимо в виде  $p = x^2 + 5y^2$ , то оно должно иметь представление  $p = 2x^2 + 2xy + 3y^2$ .] Обратите внимание на то, что эта гипотеза, по существу, утверждает, что при  $D = -5$  группа классов дивизоров состоит из двух элементов.

2. Найдите квадрат (относительно композиции) формы  $4x^2 + 9y^2$ . Найдите класс этого квадрата, подобрав собственно эквивалентную форму, которая отвечает некоторому дивизору, и возведя в квадрат соответствующий дивизор. [См. упр. 3 к § 8.1.]

## 8.7. Уравнения второй степени с двумя неизвестными

Самое общее уравнение первой степени с двумя неизвестными  $ax + by + c = 0$ , в котором коэффициенты  $a, b, c$  и искомые решения  $x$  и  $y$  являются целыми числами, можно решить при помощи алгоритма Евклида (см. упр. 1). Самое общее уравнение второй степени с двумя неизвестными  $ax^2 + bxy + cy^2 + dx + ey + f = 0$  можно решить, если выделить полные квадраты,

приведя его к виду  $\alpha x^2 + 2\beta xy + \gamma y^2 = m$ , а затем воспользоваться циклическим методом (как и в § 8.2).

Лагранж [L1] выделяет полные квадраты следующим образом. Прежде всего запишем данное уравнение в виде уравнения относительно  $x$ , коэффициенты которого являются полиномами от  $y$ , т. е.  $ax^2 + (by + d)x + (cy^2 + ey + f) = 0$ . Умножив обе части на  $4a$ , получим

$$(2ax + by + d)^2 - (by + d)^2 + 4a(cy^2 + ey + f) = 0.$$

Пусть  $t = 2ax + by + d$ ; запишем уравнение в виде  $\alpha y^2 + 2\beta y + \gamma = t^2$ , где  $\alpha = b^2 - 4ac$ ,  $\beta = bd - 2ae$  и  $\gamma = d^2 - 4af$ . Умножив обе части на  $\alpha$ , получим  $(\alpha y + \beta)^2 - \beta^2 + \alpha\gamma = \alpha t^2$ , или, проще,  $u^2 - \alpha t^2 = m$ , где

$$\alpha = b^2 - 4ac,$$

$$m = \beta^2 - \alpha\gamma = (bd - 2ae)^2 - (b^2 - 4ac)(d^2 - 4af),$$

а  $t$  и  $u$  — целые числа:

$$t = 2ax + by + d,$$

$$u = \alpha y + \beta = (b^2 - 4ac)y + bd - 2ae.$$

Каждое решение  $x, y$  исходного уравнения дает единственное решение  $t, u$  нового уравнения  $u^2 - \alpha t^2 = m$ . Обратно, решение нового уравнения получается из решения исходного уравнения тогда и только тогда, когда рациональные числа

$$y = \frac{u - \beta}{\alpha}, \quad x = \frac{1}{2a} \left[ t - b \frac{u - \beta}{\alpha} - d \right] = \frac{\alpha t - bu + b\beta - d\alpha}{2a\alpha} \quad (1)$$

являются целыми, т. е. в том и только в том случае, когда

$$u \equiv \beta \pmod{\alpha}, \quad \alpha t - bu + b\beta - d\alpha \equiv 0 \pmod{2a\alpha}. \quad (2)$$

Таким образом, общее решение данного уравнения можно найти, используя циклический метод для решения уравнения  $u^2 - \alpha t^2 = m$ , а затем отбрасывая все решения, которые не удовлетворяют сравнениям (2), и определяя  $x$  и  $y$  по формулам (1) для тех решений, которые удовлетворяют этим сравнениям.

(Если  $a = 0$ , то при  $(b, c) \neq (0, 0)$  можно при помощи обратной замены координат свести данную задачу к уравнению, в котором  $a \neq 0$ . Если  $\alpha = 0$ , то уравнение имеет простое решение — см. упр. 2.)

Этот способ пока еще нельзя считать решением нашей задачи, поскольку исключение решений  $(t, u)$ , которые не удовлетворяют сравнениям (2), требует бесконечного числа шагов. Если бы такой процесс можно было считать «решением», то нам пришлось бы считать «решением» и множество всех пар целых чисел  $(x, y)$ ,

которые остаются после исключения всех пар, не удовлетворяющих уравнению  $ax^2 + bxy + cy^2 + dx + ey + f = 0$ . Однако процесс исключения для сравнений (2) можно следующим образом свести к конечному числу шагов.

Если  $\alpha < 0$  или  $\alpha$  является квадратом и  $m \neq 0$ , то уравнение  $u^2 - \alpha t^2 = m$  имеет конечное число решений. Их можно выписать в явном виде, а затем отбросить решения, не удовлетворяющие сравнениям (2). Если  $\alpha$  является квадратом и  $m = 0$ , то существует бесконечно много решений, но все они имеют простой вид  $u = \pm kt$  ( $k^2 = \alpha$ ,  $t$  — целое) и вопрос о том, удовлетворяет ли такое решение сравнениям (2), зависит только от знака  $\pm k$  и от класса  $t$  по модулю  $2a\alpha$ . Следовательно, можно указать два (конечных) списка классов вычетов по модулю  $2a\alpha$ , таких, что общее решение имеет вид  $u = kt$ , где  $t$  принадлежит первому списку классов вычетов, или  $u = -kt$  при  $t$ , принадлежащем второму списку.

Наконец, если  $\alpha$  — положительное целое, не являющееся квадратом, то уравнение  $u^2 - \alpha t^2 = m$  либо вообще не имеет решений, либо имеет конечное число бесконечных последовательностей решений вида

$$u + t\sqrt{\alpha} = (X + Y\sqrt{\alpha})(U + T\sqrt{\alpha})^n, \quad (3)$$

где  $U + T\sqrt{\alpha}$  — основная единица,  $n$  пробегает все целые числа,  $X + Y\sqrt{\alpha}$  может быть одним из конечного числа квадратичных целых. Поэтому достаточно показать, что для любой последовательности вида (3) можно перечислить те значения  $n$ , для которых  $t$  и  $u$  удовлетворяют сравнениям (2). Так как существует только конечное число значений  $(U + T\sqrt{\alpha})^n$  по модулю  $2a\alpha$ , то должны существовать различные целые  $i$  и  $j$ , для которых  $(U + T\sqrt{\alpha})^i \equiv (U + T\sqrt{\alpha})^j \pmod{2a\alpha}$ . Единица  $U + T\sqrt{\alpha}$  имеет обратный элемент, а именно  $\pm (U - T\sqrt{\alpha})$ , поэтому  $(U + T\sqrt{\alpha})^k \equiv 1 \pmod{2a\alpha}$  при  $k = i - j$ . Следовательно, формула (3) дает значения  $t$  и  $u$ , удовлетворяющие сравнениям (2), тогда и только тогда, когда она дает такие значения при замене  $n$  на  $n + k$ . Таким образом, для того чтобы проверить все решения вида (3), достаточно проверить только те решения (3), для которых  $n = 0, 1, 2, \dots, k - 1$ .

Это завершает решение уравнения  $ax^2 + bxy + cy^2 + dx + ey + f = 0$ . По существу, приведенное здесь решение совпадает с решением Гаусса из *Disquisitiones Arithmeticae*, Art. 216. Однако Гаусс пользуется более симметричной заменой переменных для выделения полных квадратов, и это приводит к более стройным формулам.

## Упражнения

1. Решите уравнение  $ax + by + c = 0$  следующим образом. Сначала докажите, что уравнение неразрешимо, если  $c$  не делится на наибольший общий делитель  $d$  чисел  $a$  и  $b$ . Алгоритм Евклида дает  $d = au + bv$ . Воспользуйтесь этим для нахождения *одного* решения уравнения  $ax + by + c = 0$  в любом случае, когда такое уравнение имеет решение. Покажите, что разность двух решений удовлетворяет уравнению  $ar + bs = 0$ . Завершите решение задачи, найдя общее решение уравнения  $ar + bs = 0$ .

2. Сведите следующим образом решение уравнения  $ax^2 + bxy + cy^2 + dx + ey + f = 0$  к случаю  $a \neq 0$ ,  $\alpha = b^2 - 4ac \neq 0$ . Если  $a = 0$ , но  $c \neq 0$ , то, меняя  $x$  и  $y$  местами, получаем  $a \neq 0$ . Если  $a = c = 0$ , но  $b \neq 0$ , то  $x \mapsto x$ ,  $y \mapsto x + y$  — обратимая замена переменных, которая дает  $a \neq 0$ . Если  $a = b = c = 0$ , то уравнение имеет первую степень. Это показывает, что данное уравнение можно привести к виду  $\alpha y^2 + 2\beta y + \gamma = t^2$ , и при  $\alpha \neq 0$ , т. е. если уравнение не имеет вида  $2\beta y + \gamma = t^2$ , можно воспользоваться дальнейшим приведением из основного текста; здесь  $t = 2ax + by + d$ . При помощи этих двух уравнений выразите  $x$  и  $y$  через  $t$  и  $t^2$ . (Случай  $\beta = 0$  следует исключить и рассмотреть отдельно.) Покажите, что  $t$  определяет решение исходного уравнения тогда и только тогда, когда  $t + 4\alpha\beta$  определяет такое решение; заключите отсюда, что все решения исходного уравнения можно найти за конечное число шагов.

3. Напишите программу для ЭВМ, которая решает уравнение  $ax^2 + bxy + cy^2 + dx + ey + f = 0$  в целых числах при данных целых  $a, b, c, d, e, f$ . [Возможно, для выделения полного квадрата предпочтительнее пользоваться методом Гаусса.]

4. Найдите все решения уравнения  $x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$ . [Disquisitiones Arithmeticae, Art. 221.]

5. Найдите все решения уравнения  $3x^2 + 4xy - 7y^2 = 12$ . [Disquisitiones Arithmeticae, Art. 212.]

## Глава 9

### ФОРМУЛА ДИРИХЛЕ ДЛЯ ЧИСЛА КЛАССОВ

#### 9.1. Формула эйлера произведения

Эта глава посвящена формуле Дирихле для числа элементов в группах классов дивизоров из гл. 7 и 8. Конечно, в изложении Гаусса это группы классов собственной эквивалентности бинарных квадратичных форм, а групповая операция — композиция форм. Хотя Дирихле и следовал терминологии Гаусса, здесь нам удобнее рассматривать эти группы как группы классов дивизоров.

Как показано в § 6.2, основная идея, на которой основана формула Дирихле, содержится в формуле эйлера произведения

$$\sum_A \frac{1}{N(A)^s} = \prod_P \frac{1}{1 - \frac{1}{N(P)^s}}. \quad (1)$$

Здесь  $P$  пробегает все простые дивизоры, а  $A$  — все дивизоры. (Для групп классов дивизоров из гл. 8 области изменения  $P$  и  $A$  ограничиваются простыми дивизорами и теми дивизорами, которые взаимно просты с индексом рассматриваемого порядка квадратичных целых. Этому случаю посвящен § 9.6. До § 9.6 мы будем рассматривать только группы классов дивизоров полного порядка всех квадратичных целых для данного свободного от квадратов детерминанта  $D$ , т. е. группы классов дивизоров из гл. 7.)

По существу, формула эйлера произведения представляет собой новую формулировку утверждения, что любой дивизор  $A$  может быть записан одним и только одним способом в виде произведения степеней различных простых дивизоров  $P$ . В самом деле, формально

$$\frac{1}{1 - \frac{1}{N(P)^s}} = 1 + \frac{1}{N(P)^s} + \frac{1}{N(P^2)^s} + \dots \quad (2)$$

и бесконечное произведение в (1) можно разложить, выбирая слагаемое 1 во всех, за исключением конечного числа, множителях, а из остальных множителей выбирая слагаемые  $N(P^j)^{-s}$ . Настоящее доказательство формулы (1) при вещественных  $s > 1$  легко получить тем же способом, что и в § 6.3. Произведение в правой части сходится, поскольку  $\sum N(P)^{-s} \leq \sum 2p^{-s} \leq 2 \sum n^{-s} < \infty$ . Любая конечная сумма вида  $\sum N(A)^{-s}$  в левой части меньше некоторого частичного произведения из правой части; в то же время любое частичное произведение в правой части равно беско-



нечной сумме слагаемых, каждое из которых входит в левую часть (перемножение нескольких абсолютно сходящихся рядов вида (2)). Следовательно,  $\sum N(A)^{-s} \leq \prod (1 - N(P)^{-s})^{-1} \leq \sum N(A)^{-s}$ .

Как и в гл. 6, мы выведем формулу для числа классов, умножив формулу эйлера произведения на  $s - 1$  и взяв предел при  $s \downarrow 1$ . В правой части этот предел будет равен числу  $L(1, \chi)$ , что можно будет записать в виде бесконечной суммы, зависящей от  $D$ , а затем эту сумму вычислить в явном виде. Сумма в левой части разобьется на  $h$  сумм (по одной для каждого класса дивизоров), и предел при  $s \downarrow 1$  каждой из этих сумм будет одним и тем же числом. Следовательно, предел левой части равен  $h \lim_{s \downarrow 1} (s - 1) \sum N(A)^{-s}$ , где суммирование ведется по всем *главным* дивизорам  $A$ . Этот предел можно вычислить, записав его в виде суммы по квадратичным целым и заменив сумму интегралом, который находится при помощи интегрального исчисления.

Конечно, Дирихле в своем доказательстве формулы числа классов не пользовался формулой эйлера произведения в виде (1): его работа появилась даже раньше, чем теория Куммера идеальных круговых целых, не говоря уже о значительно более поздней теории идеальных квадратичных целых. Однако справедливости ради следует сказать, что формулу (1), по существу, можно найти в работе Дирихле ([D7], § 90); в ней недоставало лишь подходящего словаря, для того чтобы сформулировать (и доказать) ее в простом виде (1).

Как и при определении и изучении основных свойств числа классов, следует рассмотреть много частных случаев:  $D > 0$  или  $D < 0$ ,  $D \equiv 1$  или  $D \not\equiv 1 \pmod{4}$ ,  $D$  свободно от квадратов или  $D = t^2 D'$ . Попытка рассматривать все эти случаи единообразно не будет ни поучительной, ни полезной. Поэтому в следующих параграфах мы будем разбирать эти случаи по одному. Действительно важна лишь единая идея, заложенная в формуле (1), плюс горстка приемов, которые используются при вычислении пределов обеих частей этой формулы, умноженных на  $s - 1$ , при  $s \downarrow 1$ .

## 9.2. Первый случай

Самый простой случай формулы числа классов — это случай, когда  $D < 0$ ,  $D \not\equiv 1 \pmod{4}$  и  $D$  свободно от квадратов. В этом случае правая часть формулы эйлера произведения равна

$$\begin{aligned} \prod_P \left( 1 - \frac{1}{N(P)^s} \right)^{-1} &= \\ &= \prod_{\substack{p \text{ раз-} \\ \text{ветвляются}}} \left( 1 - \frac{1}{p^s} \right)^{-1} \prod_{\substack{p \text{ рас-} \\ \text{падаются}}} \left( 1 - \frac{1}{p^s} \right)^{-2} \prod_{\substack{p \text{ остаются} \\ \text{простыми}}} \left( 1 - \frac{1}{p^{2s}} \right)^{-1} = \end{aligned}$$

$$\begin{aligned}
&= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\substack{p \text{ рас-} \\ \text{падаются}}} \left(1 - \frac{1}{p^s}\right)^{-1} \sum_{\substack{p \text{ остаются} \\ \text{простыми}}} \left(1 + \frac{1}{p^s}\right)^{-1} = \\
&= \zeta(s) \prod_p \left(1 - \left(\frac{D}{p}\right) \frac{1}{p^s}\right)^{-1},
\end{aligned}$$

где  $\zeta(s)$  — обычная дзета-функция Римана (см. § 6.3) и где  $\left(\frac{D}{p}\right)$  равно 0, 1 или  $-1$  в зависимости от того, разветвляется, распадается или остается простым  $p$  в квадратичных целых детерминанта  $D$ . (Если  $p=2$  или  $p \mid D$ , то  $\left(\frac{D}{p}\right) = 0$ . В противном случае  $\left(\frac{D}{p}\right)$  равно символу Лежандра.)

Поскольку  $\lim_{s \downarrow 1} (s-1) \zeta(s)$  при  $s \downarrow 1$  равен 1 (см. § 6.3), предел правой части, умноженной на  $s-1$ , при  $s \downarrow 1$  равен пределу при  $s \downarrow 1$  произведения  $\prod_p \left(1 - \left(\frac{D}{p}\right) p^{-s}\right)^{-1}$ . Как было замечено в § 7.8, определение  $\left(\frac{D}{p}\right)$  можно распространить с простых целых  $p$  на все целые, взаимно простые с  $4D$ , таким образом, что  $\left(\frac{D}{n_1 n_2}\right) = \left(\frac{D}{n_1}\right) \left(\frac{D}{n_2}\right)$ . Следовательно, рассматриваемое произведение можно формально записать в виде суммы

$$\begin{aligned}
\prod_p \left(1 - \left(\frac{D}{p}\right) \frac{1}{p^s}\right)^{-1} &= \\
&= \prod_p \left(1 + \left(\frac{D}{p}\right) \frac{1}{p^s} + \left(\frac{D}{p^2}\right) \frac{1}{p^{2s}} + \dots + \left(\frac{D}{p^j}\right) \frac{1}{p^{js}} + \dots\right) = \\
&= \sum_n \left(\frac{D}{n}\right) \frac{1}{n^s},
\end{aligned}$$

где произведение берется по всем простым  $p$ , которые не делят  $4D$ , а сумма — по всем целым  $n$ , взаимно простым с  $4D$ . При  $s > 1$  это легко доказать перегруппировкой абсолютно сходящихся рядов.

В § 7.8 мы заметили также, что  $\left(\frac{D}{n}\right)$  является *характером* по модулю  $4D$ , т. е. справедливо не только соотношение  $\left(\frac{D}{n_1 n_2}\right) = \left(\frac{D}{n_1}\right) \left(\frac{D}{n_2}\right)$ , но и  $\left(\frac{D}{n+4D}\right) = \left(\frac{D}{n}\right)$ . Сумма значений этого характера равна 0 (половина классов являются распадающимися, а половина — нераспадающимися), поэтому, как и в § 6.5, можно воспользоваться суммированием по частям и доказать, что ряд  $\sum \left(\frac{D}{n}\right) n^{-s}$  условно сходится при  $s > 0$  и определяет непрерывную функцию от  $s$  при  $s > 0$ . Следовательно,

$$\lim_{s \downarrow 1} (s-1) \prod_P \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n},$$

где  $\binom{D}{n}$  считается равным 0 при  $n$ , не взаимно простом с  $4D$ , а условно сходящийся ряд в правой части суммируется в естественном порядке. По традиции это число обозначается через  $L(1, \chi)$ , где  $\chi$  — характер  $\chi(n) = \binom{D}{n}$  по модулю  $4D$ , а  $L(s, \chi) = \sum \chi(n)n^{-s}$  (как и в гл. 6).

Это завершает вычисление предела при  $s \downarrow 1$  умноженной на  $s - 1$  правой части формулы эйлерова произведения

$$\sum \frac{1}{N(A)^s} = \prod \left(1 - \frac{1}{N(P)^s}\right)^{-1}.$$

Рассмотрим теперь левую часть этой формулы. Как и в § 6.8, пределы суммы  $N(A)^{-s}$  по любым двум классам эквивалентности дивизоров  $A$  совпадают, поэтому

$$\lim_{s \downarrow 1} (s-1) \sum N(A)^{-s} = h \lim_{s \downarrow 1} (s-1) \sum_{A-\text{главные}} N(A)^{-s},$$

где  $h$  — число классов. Если  $D \neq -1$ , то имеется в точности две единицы  $\pm 1$  и каждый главный дивизор является дивизором двух и только двух квадратичных целых. Таким образом, при  $D \neq -1$

$$\sum_{A-\text{главные}} N(A)^{-s} = \frac{1}{2} \sum_{(x,y) \neq (0,0)} (x^2 - Dy^2)^{-s}.$$

При  $D = -1$  множитель  $1/2$  следует заменить на  $1/4$ . При  $s \downarrow 1$  сумма в правой части стремится к бесконечности так же, как интеграл

$$\iint_{x^2 - Dy^2 \geq 1} (x^2 - Dy^2)^{-s} dx dy.$$

Точнее, разность между этими двумя величинами остается ограниченной при  $s \downarrow 1$ . Это легко доказать (упр. 3).

Данный интеграл можно вычислить при помощи замены переменных:

$$\begin{aligned} \iint_{x^2 - Dy^2 \geq 1} (x^2 - Dy^2)^{-s} dx dy &= \\ &= \iint_{-Dz^2 - Dy^2 \geq 1} (-Dz^2 - Dy^2)^{-s} d(\sqrt{-D}z) dy = \\ &= |D|^{-s} |D|^{1/2} \iint_{z^2 + y^2 \geq |D|^{-1}} (z^2 + y^2)^{-s} dz dy = \\ &= |D|^{(1-2s)/2} \iint_{r^2 \geq |D|^{-1}} r^{-2s} r dr d\theta = \\ &= |D|^{(1-2s)/2} \cdot 2\pi \left. \frac{r^{2-2s}}{2-2s} \right|_{|D|^{-1/2}}^{\infty} = \frac{\pi}{s-1} \cdot |D|^{(1-2s)/2} |D|^{s-1}. \end{aligned}$$

Следовательно, при  $D \neq -1$

$$\lim_{s \downarrow 1} (s-1) \sum_A N(A)^{-s} = h \cdot \frac{1}{2} \cdot \lim_{s \downarrow 1} \pi \cdot |D|^{(1-2s)/2} |D|^{s-1} = \frac{h\pi}{2\sqrt{|D|}}.$$

При  $D = -1$  следует заменить в знаменателе 2 на 4.

Таким образом, если  $D < 0$ ,  $D \not\equiv 1 \pmod{4}$ ,  $D$  свободно от квадратов и  $D \neq -1$ , то

$$\frac{h\pi}{2\sqrt{|D|}} = \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n}.$$

При  $D = -1$  знаменатель 2 в левой части превращается в 4.

*Примеры.* Если  $D = -1$ , то значение  $\left(\frac{D}{n}\right)$  равно 1 при  $n \equiv 1 \pmod{4}$ ,  $-1$  при  $n \equiv 3 \pmod{4}$  и 0 при четном  $n$ . Для гауссовых целых чисел имеет место однозначность разложения на множители, поэтому число классов равно 1. Следовательно, формула для числа классов

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

совпадает с известной формулой из анализа, открытой Лейбницем. Приведенное здесь доказательство, которое основывается на свойствах разложения гауссовых целых чисел, по существу, дано Гауссом [G2, стр. 655—677]. Конечно, оно совершенно не похоже на обычное доказательство, которое сводится к обоснованию формулы  $\arctg x = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \dots$  при  $x = 1$ . Если формулу Лейбница считать известной, то формула Дирихле показывает, что  $h = 1$ <sup>1)</sup>.

При  $D = -2$  число классов равно 1 и формула Дирихле дает

$$\frac{\pi}{2\sqrt{2}} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11} - \frac{1}{13} - \dots$$

Эта замечательная формула была известна Ньютону (см. его знаменитое письмо Ольденбергу [N2] от 24 октября 1676 г.). Если

---

<sup>1)</sup> Как указал Шенкс, из формулы

$$h \frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

следует, что  $h = 1$ , ибо очевидно, что

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots < 1 < 2 \cdot \frac{\pi}{4}.$$

Следовательно, доказанная формула влечет за собой и равенство  $h = 1$ , и формулу Лейбница.

доказать формулу Ньютона другим способом, то формула Дирихле показывает, что  $h = 1$  при  $D = -2$ .

При  $D = -5$  число классов равно 2 и формула Дирихле дает

$$\frac{\pi}{\sqrt{5}} = 1 + \frac{1}{3} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} - \frac{1}{17} - \frac{1}{19} + \frac{1}{21} + \dots$$

Здесь суммирование ведется по всем целым, взаимно простым с 20; слагаемое положительно при  $n \equiv 1, 3, 7$  или  $9 \pmod{20}$  и отрицательно при  $n \equiv 11, 13, 17$  или  $19$ . Другое доказательство этой формулы, которое позволяет заключить, что  $h = 2$ , будет приведено в § 9.5.

В общем случае формула числа классов связывает  $h$  с  $\sum \binom{D}{n} \frac{1}{n} = L(1, \chi)$ . Если  $h$  известно, то эта формула дает значение  $L(1, \chi)$ . Обратно, если можно найти  $L(1, \chi)$ , то можно получить и значение  $h$ . В § 9.5 будет дан метод вычисления  $L(1, \chi)$ . В одних случаях это дает простой способ вычисления  $h$ , в других же этот способ сложнее, чем непосредственное вычисление методами гл. 7.

## Упражнения

1. При каждом  $D$  в интервале  $-5 > D > -20$ , для которого применимы рассуждения из этого параграфа, опишите явно характер  $\binom{D}{n}$  и найдите значение  $L(1, \chi)$ , вычисляя  $h$ .

2. Зависит ли  $L(1, \chi)$  от порядка суммирования ряда?

3. Докажите, что сумма значений  $(x^2 - Dy^2)^{-s}$  по всем точкам  $xy$ -плоскости с целыми коэффициентами (кроме  $x = 0, y = 0$ ) отличается от интеграла функции  $(x^2 - Dy^2)^{-s} dx dy$  по внешности эллипса  $x^2 - Dy^2 = 1$  на величину, которая остается ограниченной при  $s \downarrow 1$ . [См. § 6.12.]

4. Докажите, что в пределе при  $s \downarrow 1$  сумма значений  $N(A)^{-s}$  по классу дивизоров не зависит от выбора класса. [См. § 6.13.]

## 9.3. Второй случай

В этом параграфе мы получим формулу для числа классов дивизоров при *положительном*, свободном от квадратов и не сравнимом с 1 по модулю 4 детерминанте  $D$ . Напомним, что при  $D > 0$  определение «дивизора» требует рассмотрения  $(-1, *)$ . Следовательно, в формуле эйлерова произведения

$$\sum \frac{1}{N(A)^s} = \prod \left( 1 - \frac{1}{N(P)^s} \right)^{-1} \quad (1)$$

при  $P$ , пробегающем все простые дивизоры,  $A$  пробегает не все дивизоры, а только те, которые не содержат  $(-1, *)$ , т. е. только те дивизоры  $A$ , для которых  $N(A) > 0$ .

Точно так же как и в случае  $D < 0$  из предыдущего параграфа, получается формула

$$\lim_{s \downarrow 1} (s-1) \prod (1 - N(P)^{-s})^{-1} = \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n}.$$

Здесь функция  $\chi(n) = \left(\frac{D}{n}\right)$  является характером по модулю  $4D$ , т. е.  $\chi(n_1 n_2) = \chi(n_1) \chi(n_2)$  и  $\chi(n + 4D) = \chi(n)$ ; число в правой части этого равенства также обозначается через  $L(1, \chi)$ .

Как и раньше, получается формула

$$\lim_{s \downarrow 1} (s-1) \sum_{N(A) > 0} N(A)^{-s} = h \lim_{s \downarrow 1} (s-1) \sum_{\substack{A \text{ — главные} \\ N(A) > 0}} N(A)^{-s}. \quad (2)$$

Для этого достаточно доказать, что каждый из  $h$  классов содержит дивизоры с положительной нормой. Последнее утверждение сразу следует из замечания, что дивизор элемента  $V \bar{D}$  равен  $(-1, *) A$ , где дивизор  $A$  имеет положительную норму, так что  $(-1, *) \sim A$ , где  $N(A) > 0$ .

Для вычисления предела в правой части (2) следует, как и раньше, переписать сумму в виде суммы по квадратичным целым, а затем последнюю сумму заменить интегралом. Поэтому прежде всего мы должны для каждого главного дивизора  $A$  с  $N(A) > 0$  найти способ выбора квадратичного целого с дивизором  $A$ . Это можно сделать следующим образом.

Пусть  $\varepsilon$  — основная единица квадратичных целых детерминанта  $D$ , так что  $\varepsilon = u + vV\bar{D}$ , где  $u > 0$  и  $v > 0$ . Тогда произвольная единица имеет вид  $\pm \varepsilon^n$  ( $n$  — целое); пусть  $E = \varepsilon$  при  $N(\varepsilon) = 1$  и  $E = \varepsilon^2$  при  $N(\varepsilon) = -1$ . Если  $x + yV\bar{D}$  — квадратичное целое с дивизором  $A$ , то произвольное квадратичное целое с дивизором  $A$  можно представить в виде  $\pm E^n (x + yV\bar{D})$  ( $n$  — целое). Так как  $E = U + VV\bar{D}$ , где  $U$  и  $V$  — положительные целые, то методом из § 7.5 нетрудно доказать, что для любого данного  $x + yV\bar{D}$  коэффициенты  $x'$  и  $y'$  элемента  $x' + y'V\bar{D} = E^n (x + yV\bar{D})$  при достаточно большом  $n$  имеют одинаковые знаки (упр. 2). Следовательно, каждое квадратичное целое имеет тот же дивизор, что и некоторое квадратичное целое из «первой четверти», и для каждого главного дивизора  $A$  можно выбрать квадратичное целое  $x + yV\bar{D}$  с дивизором  $A$ , для которого  $x \geq 0$ ,  $y \geq 0$ . Как и выше, мы получаем, что  $E^n (x - yV\bar{D})$  принадлежит первой или третьей четверти при достаточно большом  $n$  (т. е. коэффициенты  $E^n (x - yV\bar{D})$  имеют одинаковый знак при большом  $n$ ), поэтому сопряженное к нему квадратичное целое  $E^{-n} (x + yV\bar{D})$



не принадлежит первой четверти при большом  $n$ . Пусть  $n$  — наименьшее положительное целое, для которого  $E^{-n}(x + y\sqrt{D})$  не принадлежит первой четверти. Тогда  $x' + y'\sqrt{D} = E^{-n+1}(x + y\sqrt{D})$  имеет тот же дивизор  $A$ , что и  $x + y\sqrt{D}$ , и принадлежит первой четверти  $x', y' \geq 0$  (действительно, либо  $n = 1$  и  $x' + y'\sqrt{D} = x + y\sqrt{D}$ , либо  $n > 1$  и  $x' + y'\sqrt{D} = E^{-(n-1)}(x + y\sqrt{D})$  принадлежит первой четверти согласно выбору  $n$ ), но  $E^{-1}(x' + y'\sqrt{D}) = E^{-n}(x + y\sqrt{D})$  первой четверти не принадлежит. Для каждого главного дивизора  $A$  существует *только одно* такое  $x' + y'\sqrt{D}$ . Действительно, если  $x' + y'\sqrt{D}$  и  $x'' + y''\sqrt{D}$  имеют один и тот же дивизор, принадлежат первой четверти и  $E^{-1}$  выводит их из первой четверти, то прежде всего  $x' + y'\sqrt{D} = \pm E^n(x'' + y''\sqrt{D})$  при некотором целом  $n$ . При необходимости меняя местами  $x' + y'\sqrt{D}$  и  $x'' + y''\sqrt{D}$ , можно считать  $n$  неотрицательным. Поэтому, поскольку все коэффициенты неотрицательны, мы получаем, что  $x' + y'\sqrt{D} = E^n(x'' + y''\sqrt{D})$  при  $n \geq 0$ . Если  $n \geq 1$ , то  $E^{-1}(x' + y'\sqrt{D}) = E^{n-1}(x'' + y''\sqrt{D})$  принадлежит первой четверти, что противоречит предположению. Следовательно,  $n = 0$ , что и требовалось показать. Таким образом, для каждого главного дивизора  $A$  найдется *одно и только одно* квадратичное целое  $x + y\sqrt{D}$  с дивизором  $A$ , которое принадлежит первой четверти ( $x, y \geq 0$ ), но которое выводится из нее умножением на  $E^{-1}$ .

Единица  $E^{-1}$  равна  $U - V\sqrt{D}$ , где  $U$  и  $V$  положительны, так что это целое  $x + y\sqrt{D}$  должно обладать тем свойством, что  $(U - V\sqrt{D})(x + y\sqrt{D})$  не принадлежит первой четверти, т. е.  $Ux - VyD$ , или  $Uy - Vx$ , или и то и другое вместе должны быть отрицательными. Если норма  $x + y\sqrt{D}$  положительна и  $Uy - Vx \geq 0$ , то  $(Uy - Vx)x \geq 0$ ,  $Uxy - Vx^2 \geq 0$ ,  $Uxy - Vx^2 + V(x^2 - Dy^2) > 0$ ,  $y(Ux - VyD) > 0$  и  $Ux - VyD > 0$ . Следовательно,  $Uy - Vx < 0$  и  $0 \leq y < (V/U)x$ . Обратно, если  $x + y\sqrt{D}$  удовлетворяет условиям  $0 \leq x$ ,  $0 \leq y < (V/U)x$ , то  $x + y\sqrt{D}$  принадлежит первой четверти, но  $E^{-1}(x + y\sqrt{D})$  первой четверти не принадлежит. Следовательно, главный дивизор  $A$  с нормой  $N(A) > 0$  является дивизором *одного и только одного* квадратичного целого  $x + y\sqrt{D}$ , для которого  $0 \leq x$  и  $0 \leq Uy < Vx$ . Таким образом,

$$\sum_{\substack{A \text{ — главный} \\ N(A) > 0}} N(A)^{-s} = \sum_{x=1}^{\infty} \sum_{0 \leq Uy < Vx} (x^2 - Dy^2)^{-s}. \quad (3)$$

Легко показать, что сумма в правой части при  $s \downarrow 1$  на ограниченную величину отличается от интеграла

$$\begin{aligned} \int \int_{\substack{0 \leq Uy < Vx \\ x^2 - Dy^1 \geq 1}} (x^2 - Dy^2)^{-s} dx dy &= \int \int_{\substack{0 \leq Uy < Vz\sqrt{D} \\ Dz^2 - Dy^2 \geq 1}} (Dz^2 - Dy^2)^{-s} d(z\sqrt{D}) dy = \\ &= D^{(-2s+1)/2} \int \int_{\substack{0 \leq Uy < Vz\sqrt{D} \\ z^2 - y^2 \geq 1/D}} (z^2 - y^2)^{-s} dz dy. \end{aligned}$$

Этот интеграл можно вычислить, используя замену переменных  $z = r \operatorname{ch} \theta$ ,  $y = r \operatorname{sh} \theta$ ,  $z^2 - y^2 = r^2$ ,  $dz dy = r dr d\theta$ . При каждом фиксированном  $r$  переменная  $\theta$  пробегает значения от 0 (где  $z = r$ ,  $y = 0$ ) до той точки, где  $Uy = Vz\sqrt{D}$ ,  $U \operatorname{sh} \theta = V\sqrt{D} \operatorname{ch} \theta$ ,  $U(e^{2\theta} - 1) = V\sqrt{D}(e^{2\theta} + 1)$ ,  $e^{2\theta}(U - V\sqrt{D}) = U + V\sqrt{D}$ ,  $e^{2\theta}E^{-1} = E$ ,  $e^{2\theta} = E^2$ ,  $\theta = \log E$ . Следовательно, этот интеграл равен

$$\begin{aligned} &= D^{(-2s+1)/2} \log E \frac{r^{2-2s}}{2-2s} \Big|_{1/\sqrt{D}}^{\infty} = \\ &= D^{(-2s+1)/2} \log E \frac{D^{s-1}}{2(s-1)}. \end{aligned}$$

Таким образом, умноженная на  $s - 1$  сумма (3) при  $s \downarrow 1$  стремится к пределу, равному  $(\log E)/2\sqrt{D}$ , и умножение обеих частей равенства (1) на  $s - 1$  с последующим переходом к пределу при  $s \downarrow 1$  дает требуемую формулу

$$\frac{h \log E}{2\sqrt{D}} = \sum_{n=1}^{\infty} \left( \frac{D}{n} \right) \frac{1}{n}.$$

Здесь  $E$  — основная единица с нормой 1, т. е.  $E = \varepsilon$ , если  $N(\varepsilon) = 1$ , и  $E = \varepsilon^2$ , если  $N(\varepsilon) = -1$ .

*Примеры.* Если  $D = 2$ , то  $\varepsilon = 1 + \sqrt{2}$ ,  $N(\varepsilon) = -1$ ,  $h = 1$  и  $\left( \frac{D}{n} \right)$  равно 1 при  $n \equiv \pm 1 \pmod{8}$ ,  $-1$  при  $n \equiv \pm 3 \pmod{8}$  и 0 при четном  $n$ . Следовательно, формула Дирихле принимает вид

$$\frac{\log(1 + \sqrt{2})}{\sqrt{2}} = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \dots$$

Если  $D = 3$ , то  $\varepsilon = 2 + \sqrt{3}$ ,  $N(\varepsilon) = 1$ ,  $h = 2$  и  $\left( \frac{D}{n} \right)$  равно 1 при  $n \equiv 1$  или  $11 \pmod{12}$ ,  $-1$  при  $n \equiv 5$  или  $7 \pmod{12}$  и 0 в остальных случаях. Следовательно,

$$\frac{\log(2 + \sqrt{3})}{\sqrt{3}} = 1 - \frac{1}{5} - \frac{1}{7} + \frac{1}{11} + \frac{1}{13} - \frac{1}{17} - \dots$$

Если  $D = 7$ , то  $\varepsilon = 8 + 3\sqrt{7} = E$ ,  $h = 2$  и формула Дирихле имеет вид

$$\frac{\log(8 + 3\sqrt{7})}{\sqrt{7}} = \sum_{n=1}^{\infty} \chi(n) \frac{1}{n},$$

где  $\chi(n) = 1$  при  $n \equiv \pm 1, \pm 3$  или  $\pm 9 \pmod{28}$ ,  $\chi(n) = -1$  при  $n \equiv \pm 5, \pm 11$  или  $\pm 13 \pmod{28}$ ,  $\chi(n) = 0$  в остальных случаях. Конечно, здесь условно сходящийся ряд  $\sum \chi(n) n^{-1}$  суммируется в естественном порядке.

### Упражнения

1. При каждом  $D$  из интервала  $7 < D < 20$ , для которого применимы рассуждения данного параграфа, найдите  $h$ ,  $E$  и  $\chi$ , входящие в формулу числа классов.

2. Пусть  $X = x + y\sqrt{D}$  — произвольное квадратичное целое и  $E$  — определенная в этом параграфе единица. Докажите, что коэффициенты  $E^n X$  имеют одинаковый знак при всех достаточно больших целых  $n$ .

3. Докажите, что сумму (3) действительно можно заменить интегралом так, как это сделано в тексте.

### 9.4. Случай $D \equiv 1 \pmod{4}$

Если  $D$  свободно от квадратов и  $D \equiv 1 \pmod{4}$ , то квадратичные целые  $x + y\sqrt{D}$  могут содержать 2 в знаменателях; точнее, 2 делит  $1 - \sqrt{D}$  и каждое квадратичное целое можно записать в виде  $u + v \cdot \frac{1}{2}(1 - \sqrt{D})$  с целыми  $u$  и  $v$ . В этом случае простое 2 не разветвляется. Действительно (см. § 7.1), 2 распадается, если  $D \equiv 1 \pmod{8}$ , и остается простым, если  $D \equiv 5 \pmod{8}$ . Таким образом, характер  $\chi(n) = \left(\frac{D}{n}\right)$  больше не обращается в нуль при всех четных  $n$ , и, как легко показать,  $\chi(n)$  равно нулю тогда и только тогда, когда  $n$  не взаимно просто с  $D$ . Кроме того,  $\chi$  является характером по модулю  $D$ , т. е.  $\chi(mn) = \chi(m)\chi(n)$  и  $\chi(n + D) = \chi(n)$ . При таком  $\chi$  по-прежнему справедлива формула

$$\lim_{s \downarrow 1} (s-1) \prod_P (1 - N(P)^{-s})^{-1} = \prod_{p \nmid D} \left(1 - \left(\frac{D}{p}\right) \frac{1}{p}\right)^{-1} = L(1, \chi).$$

В другой части равенства предел  $\lim (s-1) \sum N(A)^{-s}$  можно найти точно так же, как и раньше; нужно только учесть, что квадратичные целые  $x + y\sqrt{D}$ , рассматриваемые как точки  $xu$ -плоскости, имеют удвоенную плотность (в каждом квадрате  $\{(x, y): x_0 \leq x < x_0 + 1, y_0 \leq y < y_0 + 1\}$  содержатся ровно 2 квадратичных целых), так что соответствующий интеграл

удваивается. Поэтому при  $D \equiv 1 \pmod{4}$  формула числа классов принимает следующий вид: при  $D < 0$

$$h \frac{\pi}{\sqrt{|D|}} = L(1, \chi)$$

(кроме  $D = -3$ , когда вместо двух единиц имеется шесть, поэтому левая часть этой формулы превращается в  $h\pi/3\sqrt{3}$ ), а при  $D > 0$

$$h \frac{\log E}{\sqrt{D}} = L(1, \chi)$$

(здесь  $E$  — основная единица  $\varepsilon$ , если  $N(\varepsilon) = 1$ , и  $E = \varepsilon^2$ , если  $N(\varepsilon) = -1$ ).

Например, при  $D = -3$  формула Дирихле превращается в

$$\frac{\pi}{3\sqrt{3}} = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \dots$$

Эта формула приведена Эйлером в работе *Introductio in Analysin Infinitorum* [Е6, § 176]. (Я не знаю, была ли эта формула известна кому-нибудь до Эйлера.) При  $D = -7$  получаем

$$1 \cdot \frac{\pi}{\sqrt{7}} = 1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{8} + \dots$$

Действительно, в этом случае  $\chi(n) = 0$ , если  $n \equiv 0 \pmod{7}$ ,  $\chi(n) = 1$ , если  $n \equiv 1, 2$  или  $4 \pmod{7}$ ,  $\chi(n) = -1$ , если  $n \equiv 3, 5$  или  $6$ , и число классов равно 1 (2 разлагается на настоящие множители  $\frac{1}{2}(1 \pm \sqrt{-7})$ , а 3 и 5 остаются простыми).

Если  $D = 5$ , то  $\varepsilon = \frac{1}{2}(1 + \sqrt{5})$ ,  $E = \varepsilon^2$ ,  $h = 1$  (как 2, так и 3 остаются простыми), и формула Дирихле дает

$$\frac{2 \log \frac{1}{2}(1 + \sqrt{5})}{\sqrt{5}} = 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \dots$$

Если  $D = 13$  (конечно, не следует рассматривать случай  $D = 9$ ), то  $\varepsilon = \frac{1}{2}(3 + \sqrt{13})$ ,  $E = \varepsilon^2$ ,  $h = 1$  (2, 5, 7 и 11 остаются простыми, а 3 разлагается на настоящие множители:  $3 = (4 - \sqrt{13}) \times (4 + \sqrt{13})$ ), и мы получаем формулу

$$\frac{2 \log \frac{1}{2}(3 + \sqrt{13})}{\sqrt{13}} = \sum_{13 \nmid n} \pm \frac{1}{n};$$

здесь слагаемые  $\pm \frac{1}{n}$  положительны при  $n \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$  и отрицательны при  $n \equiv \pm 2, \pm 5, \pm 6 \pmod{13}$ . Разумеется, условно сходящийся ряд  $\sum \pm (1/n)$  следует суммировать в естественном порядке.

### Упражнения

1. Найдите формулу числа классов при  $D = -23$ .
2. Найдите формулу числа классов при  $D = 65$ .

### 9.5. Вычисление суммы $\sum \left(\frac{D}{n}\right) \frac{1}{n}$

Если мы хотим пользоваться формулой числа классов для нахождения числа классов  $h$ , то следует найти независимый способ вычисления суммы

$$L(1, \chi) = \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n}.$$

Здесь  $\chi$  — характер по модулю  $4D$  (или по модулю  $D$ , если  $D \equiv 1 \pmod{4}$ ), определенный соотношениями  $\chi(n_1 n_2) = \chi(n_1) \chi(n_2)$  и

$$\chi(p) = \begin{cases} 0, & \text{если } p \text{ разветвляется,} \\ 1, & \text{если } p \text{ распадается,} \\ -1, & \text{если } p \text{ остается простым,} \end{cases}$$

в квадратичных целых для свободного от квадратов детерминанта  $D$ . В табл. 9.5.1 приведены значения  $\chi(n)$  при  $|D| \leq 7$  и  $1 \leq n \leq 28$ .

Пусть  $m = |4D|$ , если  $D \not\equiv 1 \pmod{4}$ , и  $m = |D|$ , если  $D \equiv 1 \pmod{4}$ . Тогда  $\chi$  является характером по модулю  $m$ , и рассуждения из § 6.5 показывают, что  $L(1, \chi)$  можно записать в виде

$$L(1, \chi) = c_1 \log \frac{1}{1-\alpha} + c_2 \log \frac{1}{1-\alpha^2} + \dots + c_m \log \frac{1}{1-\alpha^m}, \quad (1)$$

где  $\alpha$  — примитивный корень  $m$ -й степени из единицы и через  $\log(1/(1-z))$  обозначена функция, определенная рядом  $\sum (z^n/n)$  (при суммировании в естественном порядке) для всех комплексных чисел  $|z| \leq 1$ , кроме  $z = 1$ , а

$$c_j = \frac{1}{m} [\chi(1) \alpha^{-j} + \chi(2) \alpha^{-2j} + \dots + \chi(m) \alpha^{-mj}]. \quad (2)$$

Здесь  $c_m = 0$  (сумма всех значений характера  $\chi$  равна нулю, поскольку половина классов по модулю  $m$  являются распадающимися, а вторая половина — нераспадающимися), и расходящийся ряд  $\log(1/(1-\alpha^m))$  фактически не входит в формулу (1).

Таблица 9.5.1. (Ср. с табл. 7.8.1.)

$D$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$-1$	+	0	−	0	+	0	−	0	+	0	−	0	+	0
$-2$	+	0	+	0	−	0	−	0	+	0	+	0	−	0
$-3$	+	−	0	+	−	0	+	−	0	+	−	0	+	−
$-5$	+	0	+	0	0	0	+	0	+	0	−	0	−	0
$-6$	+	0	0	0	+	0	+	0	0	0	+	0	−	0
$-7$	+	+	−	+	−	−	0	+	+	−	+	−	−	0
2	+	0	−	0	−	0	+	0	+	0	−	0	−	0
3	+	0	0	0	−	0	−	0	0	0	+	0	+	0
5	+	−	−	+	0	+	−	−	+	0	+	−	−	+
6	+	0	0	0	+	0	−	0	0	0	−	0	−	0
7	+	0	+	0	−	0	0	0	+	0	−	0	−	0

$D$	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$-1$	−	0	+	0	−	0	+	0	−	0	+	0	−	0
$-2$	−	0	+	0	+	0	−	0	−	0	+	0	+	0
$-3$	0	+	−	0	+	−	0	+	−	0	+	−	0	+
$-5$	0	0	−	0	−	0	+	0	+	0	0	0	+	0
$-6$	0	0	−	0	−	0	0	0	−	0	+	0	0	0
$-7$	+	+	−	+	−	−	0	+	+	−	+	−	−	0
2	+	0	+	0	−	0	−	0	+	0	+	0	−	0
3	0	0	−	0	−	0	0	0	+	0	+	0	0	0
5	0	+	−	−	+	0	+	−	−	+	0	+	−	−
6	0	0	−	0	+	0	0	0	+	0	+	0	0	0
7	−	0	−	0	+	0	0	0	−	0	+	0	+	0



Функцию  $\log (1/(1-z))$  можно вычислить при помощи формулы (7) из § 6.5, следовательно, эти две формулы суммируют бесконечный ряд  $L(1, \chi)$  и сводят его нахождение к конечному числу шагов.

Дальнейшие упрощения при вычислении  $L(1, \chi)$  можно сделать при помощи следующей замечательной теоремы: *преобразование Фурье*  $(c_1, c_2, \dots, c_m)$  характера  $(\chi(1), \chi(2), \dots, \chi(m))$  кратно  $(\chi(1), \chi(2), \dots, \chi(m))$ . Именно, если  $c_j$  определены соотношением (2), то существует такое число  $\mu$ , что  $c_j = \mu \chi(j)$  при  $j = 1, 2, \dots, m$ . Эту теорему можно доказать следующим образом. Если  $j$  взаимно просто с  $m$ , то существует такое целое  $k$ , что  $jk \equiv 1 \pmod{m}$  и

$$\begin{aligned} c_1 &= \frac{1}{m} [\chi(1) \alpha^{-1} + \chi(2) \alpha^{-2} + \dots + \chi(m) \alpha^{-m}] = \\ &= \frac{1}{m} [\chi(jk) \alpha^{-jk} + \chi(2jk) \alpha^{-2jk} + \dots + \chi(mjk) \alpha^{-mjk}] = \\ &= \chi(j) \cdot \frac{1}{m} [\chi(k) \alpha^{-jk} + \chi(2k) \alpha^{-2jk} + \dots + \chi(mk) \alpha^{-mjk}] = \\ &= \chi(j) \cdot \frac{1}{m} [\chi(1) \alpha^{-j} + \chi(2) \alpha^{-2j} + \dots + \chi(m) \alpha^{-jm}] = \\ &= \chi(j) c_j \end{aligned}$$

(поскольку  $k, 2k, \dots, mk$  — система представителей по модулю  $m$ ). Так как  $\chi(j) = \pm 1$ , то отсюда следует, что  $c_j = \chi(j) c_1$ , и при  $\mu = c_1$  мы получаем, что  $c_j = \mu \chi(j)$  для  $j$ , взаимно простого с  $m$ . При  $j$ , не взаимно простом с  $m$ ,  $\chi(j) = 0$ , поэтому для доказательства теоремы необходимо и достаточно доказать, что  $c_j = 0$ , если  $j$  не взаимно просто с  $m$ . Пусть  $j = rv$ , где  $r$  — простой делитель  $m$ , скажем  $m = rq$ . Тогда

$$c_j = \frac{1}{m} [\chi(1) \alpha^{-rv} + \chi(2) \alpha^{-2rv} + \dots + \chi(m) \alpha^{-mrv}].$$

Если  $rv \equiv sv \pmod{q}$ , то  $\alpha^{-rv} = \alpha^{-sv}$  и  $c_j$  равно сумме  $q$  слагаемых:

$$\begin{aligned} c_j &= \frac{1}{m} \left[ \left( \sum_{t \equiv 1 \pmod{q}} \chi(t) \right) \alpha^{-rv} + \right. \\ &\quad \left. + \left( \sum_{t \equiv 2} \chi(t) \right) \alpha^{-2rv} + \dots + \left( \sum_{t \equiv 0} \chi(t) \right) \alpha^{-mrv} \right]. \end{aligned}$$

Поэтому теорема будет доказана, если показать, что эти суммы по классам вычетов по модулю  $q$  равны нулю, т. е. если показать, что сумма значений  $\chi$  по  $r$  целым числам  $t$ , принадлежащим одному классу вычетов по модулю  $q$ ,  $0 \leq t < m$ , равна нулю. Такое свойство характеров  $\chi(j) = \binom{D}{j}$  легко доказать, используя фор-

мулы для  $\binom{D}{j}$  из § 7.8 (упр. 1). Это завершает доказательство теоремы.

Легко вычислить константу  $\mu$  (по крайней мере с точностью до знака). Для этого нужно лишь заметить, что

$$\begin{aligned}\chi(j) &= c_1 \alpha^j + c_2 \alpha^{2j} + \dots + c_m \alpha^{mj} = \\ &= \mu [\chi(1) \alpha^j + \chi(2) \alpha^{2j} + \dots + \chi(m) \alpha^{mj}] = \\ &= \mu \sum_{v=1}^m \chi(v) \alpha^{vj}.\end{aligned}$$

Подставив  $\chi(j)$ , выраженное правой частью этой формулы, в саму эту правую часть, получим

$$\begin{aligned}\chi(j) &= \mu \sum_{v=1}^m \left[ \mu \sum_{\lambda=1}^m \chi(\lambda) \alpha^{\lambda v} \right] \alpha^{vj} = \\ &= \mu^2 \sum_{\lambda=1}^m \left[ \sum_{v=1}^m \alpha^{\lambda v} \alpha^{jv} \right] \chi(\lambda).\end{aligned}$$

Внутренняя сумма равна нулю, если  $\lambda + j \not\equiv 0 \pmod{m}$ ; в противном случае эта сумма равна  $m$ . [Каждая степень  $\alpha$ , отличная от 1, является корнем многочлена  $1 + x + x^2 + \dots + x^{m-1} = (1 - x^m)/(1 - x)$ .] Следовательно,  $\chi(j) = \mu^2 m \chi(-j) = \chi(j) \mu^2 m \chi(-1)$  и

$$\mu = \pm \frac{1}{\sqrt{\chi(-1) m}}.$$

Используя эти свойства коэффициентов  $c_j$  в (1), получаем

$$L(1, \chi) = \pm \frac{1}{\sqrt{\chi(-1) m}} \sum_{j=1}^m \chi(j) \log \frac{1}{1 - \alpha^j}. \quad (3)$$

Неопределенность в знаке перед суммой не доставляет затруднений, поскольку формула

$$L(1, \chi) = \lim_{s \downarrow 1} (s-1) \prod_P \left( 1 - \frac{1}{N(P)^s} \right)^{-1}$$

показывает, что  $L(1, \chi) \geq 0$ . При дальнейшем приведении формулы для  $L(1, \chi)$  естественно случаи  $D < 0$  и  $D > 0$  рассматривать отдельно.

*Случай 1:*  $D < 0$ . Здесь  $\chi(-1) = -1$ , и вещественные части логарифмов в (3) сокращаются. Мнимые части можно найти при помощи формулы

$$\log \frac{1}{1 - e^{i\theta}} = -\log \left( 2 \sin \frac{\theta}{2} \right) + \frac{i}{2} (\pi - \theta)$$

( $0 < \theta < 2\pi$ ) из § 6.5. Тогда при  $\alpha = e^{2\pi i/m}$  получаем

$$\begin{aligned} L(1, \chi) &= \pm \frac{1}{i \sqrt{m}} \cdot \frac{i}{2} \cdot \sum_{j=1}^m \chi(j) \left( -\frac{2\pi j}{m} \right) + \text{const} \sum_{j=1}^m \chi(j) = \\ &= \pm \frac{\pi}{m \sqrt{m}} \sum \chi(j) j. \end{aligned}$$

Так как  $L(1, \chi) \geq 0$ , то окончательная формула имеет вид

$$L(1, \chi) = \frac{\pi}{m \sqrt{m}} |1 + \chi(2) 2 + \chi(3) 3 + \dots + \chi(m) m|. \quad (4)$$

Это число сравнительно просто вычислить при любом заданном  $D < 0$ .

*Примеры.* При  $D = -1$  имеем  $m = 4$  и

$$L(1, \chi) = \frac{\pi}{4 \sqrt{4}} |1 - 3| = \frac{\pi}{4}$$

— формула Лейбница. Если  $D = -2$ , то  $m = 8$ , и мы получаем формулу Ньютона из § 9.2:

$$L(1, \chi) = \frac{\pi}{8 \sqrt{8}} |1 + 3 - 5 - 7| = \frac{\pi}{2 \sqrt{2}}.$$

Если  $D = -3$ , то  $m = 3$  и

$$L(1, \chi) = \frac{\pi}{3 \sqrt{3}} |1 - 2| = \frac{\pi}{3 \sqrt{3}},$$

как было указано в предыдущем параграфе. При  $D = -5$

$$L(1, \chi) = \frac{\pi}{20 \sqrt{20}} |1 + 3 + 7 + 9 - 11 - 13 - 17 - 19| = \frac{\pi}{\sqrt{5}};$$

если  $D = -7$ , то  $L(1, \chi) = \pi (7 \sqrt{7})^{-1} |1 + 2 - 3 + 4 - 5 - 6| = \pi/\sqrt{7}$ , и т. д. Некоторые интересные упрощения этой формулы приведены в упражнениях (см. резюме в конце упражнений).

*Случай 2:  $D > 0$ .* Здесь  $\chi(-1) = 1$  и мнимые части логарифмов в формуле (3) сокращаются. Вещественные части равны  $-\log 2 - \log(\sin(\theta/2))$ , и  $\log 2$  не вносит вклада в сумму, поскольку  $\sum \chi(j) = 0$ . Следовательно,

$$L(1, \chi) = \pm \frac{1}{\sqrt{m}} \log \left| \frac{\prod \sin \frac{\pi j}{m}}{\prod \sin \frac{\pi j}{m}} \right|.$$

где в числителе  $j$  пробегает все целые между 0 и  $m$ , для которых  $\chi(j) = 1$ , а в знаменателе — все такие целые, для которых  $\chi(j) = -1$ . В этом случае найти явное выражение для  $L(1, \chi)$  значительно труднее, чем при  $D < 0$ .

*Примеры.* Если  $D = 2$ , то  $m = 8$  и

$$L(1, \chi) = \pm \frac{1}{2\sqrt{2}} \log \frac{\sin \frac{\pi}{8} \sin \frac{7\pi}{8}}{\sin \frac{3\pi}{8} \sin \frac{5\pi}{8}}.$$

Это выражение можно вычислить явно, положив  $x = \sin(\pi/8)$  и  $y = \sin(3\pi/8) = \cos(\pi/8)$ . Тогда  $x^2 + y^2 = 1$ ,  $-x^2 + y^2 = \cos 2(\pi/8) = \sqrt{2}/2$ ,  $2y^2 = 1 + (\sqrt{2}/2) = (2 + \sqrt{2})/2$ ,  $2x^2 = (2 - \sqrt{2})/2$ ,  $L(1, \chi) = \pm (2\sqrt{2})^{-1} \cdot \log(x^2/y^2) = \pm (2\sqrt{2})^{-1} \times \log[(2 - \sqrt{2})/(2 + \sqrt{2})] = \log[(2 + \sqrt{2})^2/2]/2\sqrt{2} = \log(1 + \sqrt{2})/\sqrt{2}$ , что совпадает с выражением из § 9.3.

Аналогично, при  $D = 3$  формула Дирихле дает

$$\begin{aligned} L(1, \chi) &= \pm \frac{1}{2\sqrt{3}} \log \frac{\sin \frac{\pi}{12} \sin \frac{11\pi}{12}}{\sin \frac{5\pi}{12} \sin \frac{7\pi}{12}} = \\ &= \pm \frac{1}{2\sqrt{3}} \log \frac{2x^2}{2y^2} = \pm \frac{1}{2\sqrt{3}} \log \frac{1 - \frac{\sqrt{3}}{2}}{1 + \frac{\sqrt{3}}{2}} = \\ &= \frac{1}{2\sqrt{3}} \log \frac{2 + \sqrt{3}}{2 - \sqrt{3}} = \frac{1}{2\sqrt{3}} \log \frac{(2 + \sqrt{3})^2}{1} = \frac{\log(2 + \sqrt{3})}{\sqrt{3}}, \end{aligned}$$

где  $x = \sin(\pi/12)$  и  $y = \sin(5\pi/12)$ .

При  $D = 5$  удобнее оставить формулу в виде (3), заметив, что ее мнимая часть равна нулю. Тогда, используя вычисления из § 6.5, находим

$$\begin{aligned} L(1, \chi) &= \pm \frac{1}{\sqrt{5}} \log \frac{(1 - \alpha^2)(1 - \alpha^3)}{(1 - \alpha)(1 - \alpha^4)} = \\ &= \frac{1}{\sqrt{5}} \log \frac{3 + \sqrt{5}}{2} = \frac{2}{\sqrt{5}} \log \frac{1 + \sqrt{5}}{2}. \end{aligned}$$

Эта формула была также выведена в § 6.5 и 9.4.

При  $D = 7$  ни один из этих методов не приводит к очень удобному вычислению значения  $L(1, \chi) = \log(8 + 3\sqrt{7})/\sqrt{7}$ , которое мы нашли в § 9.3 при помощи прямого вычисления  $h$  и формулы числа классов.

## Упражнения

1. Предположим, что  $D$  свободно от квадратов. Пусть  $m = |D|$  или  $|4D|$  — в зависимости от того, сравнимо  $D$  с 1 по модулю 4 или нет. Предположим, что  $m = pq$ , где  $p$  — простое. Докажите, что тогда сумма  $\binom{D}{t}$  по  $p$  целым значениям  $t$ ,  $0 \leq t < m$ , принадлежащим одному классу вычетов по модулю  $q$ , равна нулю. [Пусть  $\binom{D}{n} = \binom{\sigma}{n} \binom{n}{p_1} \binom{n}{p_2} \cdots \binom{n}{p_\mu} \binom{n}{p'_1} \times \cdots \times \binom{n}{p'_2} \cdots \binom{n}{p'_\nu}$ , где  $D = (-1)^\delta 2^\varepsilon p_1 p_2 \cdots p_\mu p'_1 p'_2 \cdots p'_\nu$ ,  $\delta$  и  $\varepsilon$  равны 0 или 1, простые  $p$  сравнимы с 1 по модулю 4, а  $p'$  сравнимы с 3 по модулю 4,  $\sigma = (-1)^{\delta+\nu} 2^\varepsilon \equiv D \pmod{4}$  и  $\binom{\sigma}{n} = 1$  при  $\sigma = 1$ , а  $\binom{\delta}{n} = 0$  при  $\sigma \neq 1$  и четном  $n$ . Если  $p \mid m$  и  $p$  нечетно, то все, кроме одного, множители в  $\binom{D}{n}$  имеют то же значение при  $n \pm q$ , что и при  $n$ . (Если  $2 \mid \sigma$ , то  $8 \mid q$ . Если  $\sigma = -1$ , то  $4 \mid q$ .) Следовательно, искомая сумма постоянным множителем отличается от суммы значений  $\binom{t}{p}$ , которая равна нулю. Если  $p \mid m$  и  $p = 2$ , рассмотрите два случая. При  $\varepsilon = 1$  число  $q$  равно учетверенному нечетному целому и  $\binom{\delta}{n} = -\binom{\sigma}{n+q}$  ( $\sigma = \pm 2$ ), а остальные множители в  $\binom{D}{n}$  одинаковы при  $n$  и  $n \pm q$ . Если  $\varepsilon = 0$ , то  $D \not\equiv 1 \pmod{4}$ ,  $q \equiv 2 \pmod{4}$  и снова первый множитель меняет знак, а остальные остаются неизменными.]

2. При  $D = -1$  найдите коэффициенты  $s$  и покажите, что вычисление  $L(1, \chi)$ , приведенное в данном параграфе, сводится к вычислению  $-i \log \left( \frac{1}{2} \sqrt{2} + \frac{1}{2} \sqrt{2} i \right)$ , т. е. к нахождению  $\arctg 1$ .

3. При  $D < 0$  и  $D \equiv 1 \pmod{4}$  вычисление  $L(1, \chi)$  по формуле (4) можно упростить следующим образом. Слагаемые в полученной сумме можно таким образом сгруппировать попарно, что она становится суммой по множеству  $1, 2, \dots, \frac{1}{2}(|D| - 1)$ , или их можно так разбить на пары, что получится сумма по множеству  $2, 4, \dots, |D| - 1$ . Это дает два выражения данной суммы через  $\Sigma = \binom{D}{1} + \binom{D}{2} + \cdots + \binom{D}{\nu}$  и  $\Sigma' = \binom{D}{1} + \binom{D}{2} 2 + \cdots + \binom{D}{\nu} \nu$ , где  $\nu = (|D| - 1)/2$ . Этими выражениями можно воспользоваться и исключить  $\Sigma'$ . Отсюда следует, что  $h = |\Sigma|$  при  $\binom{D}{2} = +1$  или  $D = -3$  и  $h = \frac{1}{3} |\Sigma|$  при  $\binom{D}{2} = -1$  и  $D \neq -3$ . Восполните детали доказательства этой теоремы.

4. Используя метод из упр. 3, вычислите  $h$  при  $D = -7, -11, -15, -19, -23, -31, -35, -39, -43, -47$ . Это хорошее упражнение для развития навыков вычисления  $\binom{D}{n}$ . В таких вычислениях можно добиться значительной экономии. Редко, если вообще когда-нибудь, возникает необходимость вычислять символы Лежандра, отличные от тривиальных  $\binom{D}{2}$ ,  $\binom{D}{3}$  и  $\binom{D}{5}$ .

5. Покажите, что если  $D$  отрицательно, свободно от квадратов и не сравнимо с 1 по модулю 4, причем  $D \neq -1$ , то  $h = |\Sigma|$ , где  $\Sigma$  равно сумме  $\binom{D}{n}$  по всем  $n$  из промежутка  $1 \leq n < |D|$ . [Воспользуйтесь формулами  $\chi(n + 2D) = -\chi(n)$  и  $\chi(4D - n) = -\chi(n)$ .] В этих случаях вычислять  $\binom{D}{n}$  утомительнее. Дальнейшие упрощения приведены в следующих ниже упражнениях. По этой формуле вычислите  $h$  при  $D = -5, -6, -10, -13, -14, -17, -21$ .

6. Пусть  $D$  отрицательно, свободно от квадратов и сравнимо с  $-1$  по модулю 4. Вычисление числа классов методом из упр. 5 требует больше и более трудных вычислений символа Лежандра, чем следующий остроумный метод Дирихле. (См. [D7], разд. 106.) Пусть  $D = -P$ , где  $P$  — положительное число (не обязательно простое), сравнимое с 1 по модулю 4. Кроме того, предположим, что  $P \neq 1$ . Тогда  $\binom{D}{n} = \binom{-1}{n} \binom{n}{P}$ , где  $\binom{n}{P}$  равно произведению  $\binom{n}{p_i}$  по простым делителям  $p_i$  (обязательно различным) числа  $P$ . Для целых чисел  $r$  определим  $\Psi(r)$  формулой

$$\Psi(r) = \sum_{s=1}^{P-1} \binom{s}{P} \log \frac{1}{1 - i^r \gamma^s},$$

где  $\gamma = e^{2\pi i/P}$  и  $\log$  определен рядом  $\log(1/(1-z)) = \sum z^n/n$  (поэтому мнимая часть логарифма заключена между  $-\pi/2$  и  $\pi/2$ ). Тогда формула (3) показывает, что  $L(1, \chi) = \pm i m^{-1/2} [0 \cdot \Psi(0) + 1 \cdot \Psi(1) + 0 \cdot \Psi(2) + (-1) \Psi(3)]$ . Действительно, каждый корень  $m$ -й степени из единицы можно единственным способом записать в виде  $i^r \gamma^s$ ,  $r = 0, 1, 2, 3$ ;  $s = 0, 1, 2, \dots, P-1$ . Таким образом,  $h = \pm i \pi^{-1} [\Psi(1) - \Psi(3)]$ . Положим  $K(r) = \Psi(r) - \Psi(-r)$ . Тогда  $h = \pm i \pi^{-1} K(1)$ . Тождество  $K(r) = \sum \binom{s}{P} \log [(1 - i^{-r} \gamma^{-s}) / (1 - i^r \gamma^s)]$  показывает не только, что  $K(r)$  — чисто мнимое число, но и что оно равно  $-\sum \binom{s}{P} (2\pi i k / 4P)$ , где  $k$  — целое число, определенное условиями  $0 < k < 4P$ ,  $k \equiv Pr + 4s$ . Следовательно, при  $r = 0, 1, 2, 3$  разность  $K(r+1) - K(r)$  равна сумме слагаемых вида  $-\binom{s}{P} (2\pi i P / 4P)$ , за исключением случая, когда  $s$  удовлетворяет неравенствам  $Pr + 4s < 4P \leq P(r+1) + 4s$ ; в последнем случае это слагаемое равно  $-\binom{s}{P} (2\pi i (P - 4P) / 4P)$ . (Обратите внимание на сходство этого рассуждения с рассуждениями Куммера из § 6.16.) Следовательно,  $K(r+1) - K(r) = 2\pi i \sum \binom{s}{P}$ , где суммирование проводится по всем значениям  $s$ , для которых  $Pr + 4s < 4P \leq P(r+1) + 4s$ . Это выражение представляет собой сумму по четвертой части всех целых  $1, 2, \dots, P-1$ . В частности, если через  $Q_j$ ,  $j = 1, 2, 3, 4$ , обозначить сумму  $\binom{s}{P}$  по  $j$ -й четверти  $(j-1)(P-1)/4 < s \leq j(P-1)/4$ , то  $K(r+1) - K(r) = 2\pi i Q_{4-r}$ . Но  $K(3) = -K(1)$ , поэтому  $K(1) = 1/2 [K(1) - K(3)] = -1/2 [K(3) - K(2) + K(2) - K(1)] = -1/2 [2\pi i Q_2 + 2\pi i Q_3]$ . Поскольку  $Q_1 + Q_2 + Q_3 + Q_4 = 0$  и  $Q_1 = Q_4$ , отсюда следует, что  $K(1) = 2\pi i Q_1$ . Таким образом,  $h = \pm 2Q_1$ . Используйте эту формулу для нахождения  $h$  при  $D = -5, -13, -17, -21, -29, -33, -37, -41, -53$ .

7. Дирихле<sup>1)</sup> получил упрощения формулы числа классов, подобные сделанным в упр. 6, также и в остальных случаях свободного от квадратов и отрицательного детерминанта  $D$ . В этом упражнении мы рассмотрим  $D \equiv 2 \pmod{8}$ , а следующее упражнение будет посвящено единственному оставшемуся случаю  $D \equiv -2 \pmod{8}$ . Пусть  $D \equiv 2 \pmod{8}$ . Предположим, что  $D = -2P$ , где  $P \equiv -1 \pmod{4}$  и  $P$  равно произведению различных нечет-

<sup>1)</sup> Судя по предисловию Дедекинда к первому изданию книги [D7], он сам, вероятно, сделал в этом направлении уж никак не меньше, чем Дирихле.



ных простых. Тогда  $\binom{D}{n} = \binom{2}{n} \binom{n}{P}$ , где  $\binom{n}{P}$  определено так же, как и раньше. Пусть  $\beta = e^{2\pi i/8}$ ,  $\gamma = e^{2\pi i/P}$  и

$$\Psi(r) = \sum_{s=1}^{P-1} \binom{s}{P} \log \frac{1}{1 - \beta^r \gamma^s}.$$

Тогда  $h = \pm i\pi^{-1} [\Psi(1) - \Psi(3) - \Psi(5) + \Psi(7)]$ . Пусть  $K(r) = \Psi(r) + \Psi(-r)$ . Тогда  $K(r) = -\sum \binom{s}{P} (2\pi i k/8P)$ , где  $k \equiv Pr + 8s \pmod{8P}$  и  $0 \leq k < 8P$ . Следовательно, при  $r = 0, 1, \dots, 7$  справедливо равенство  $K(r+1) - K(r) = 2\pi i C$ , где  $C$  равно сумме  $\binom{s}{P}$  по всем значениям  $s$ , для которых  $Pr + 8s < 8P \leq P(r+1) + 8s$ . Пусть  $C_j$  — сумма  $\binom{s}{P}$  по всем  $s$ , принадлежащим  $j$ -му «октанту»  $(j-1)/8 < s/P < j/8$ . Тогда  $K(r+1) - K(r) = 2\pi i C_{8-r}$ . Это дает  $h = \pm i\pi^{-1} [K(1) - K(3)] = \pm i\pi^{-1} [K(3) - K(2) + K(2) - K(1)] = \pm 2 [C_6 + C_7] = \pm 2 [C_2 + C_3]$ . Используйте эту формулу для нахождения  $h$  при  $D = -6, -14, -22, -30, -38$ .

8. Наконец, рассмотрим случай  $D \equiv -2 \pmod{8}$ . Пусть  $D = -2P$ ,  $P \equiv 1 \pmod{4}$ ,  $P \neq 1$ . Определите  $\Psi(r)$  так же, как и выше, и докажите, что  $h = \pm i\pi^{-1} [\Psi(1) + \Psi(3) - \Psi(5) - \Psi(7)]$ . Если  $K(r) = \Psi(r) - \Psi(-r)$ , то  $K(r+1) - K(r) = 2\pi i C_{8-r}$ , где  $C_j$  равно сумме  $\binom{s}{P}$  по  $j$ -му «октанту» и  $h = \pm i\pi^{-1} [K(1) + K(3)]$ . Вычисление  $K(1) + K(3)$  как будто бы требует еще одного тождества, а именно  $K(r) + K(r+4) = \binom{2}{P} K(2r)$ . Это следует из аналогичного тождества для  $\Psi$ , которое в свою очередь получается из соотношения  $\log(1/(1-\alpha)) + \log(1/(1+\alpha)) = \log(1/(1-\alpha^2))$ . (Последнее тождество несколько менее очевидно, чем это может показаться, из-за многозначности мнимой части логарифма. Тем не менее его можно доказать из общих соображений — не прибегая к вычислениям.) Тогда, если  $\binom{2}{P} = 1$ , то  $K(1) + K(5) = K(2)$ ,  $K(3) + K(7) = K(6)$ ,  $K(1) + K(3) = K(2) - K(5) + K(6) - K(7)$ , следовательно,  $h = \pm 2 [C_1 - C_4]$ . Если  $\binom{2}{P} = -1$ , то  $3K(1) + 3K(3) = K(1) - K(2) + K(1) - K(5) + K(3) - K(6) + K(3) - K(7)$ , и снова  $h = 2 |C_1 - C_4|$ . Используйте эту формулу для вычисления  $h$  при  $D = -10, -26, -34, -42$ .

9. Всякий, кто провел вычисления из предыдущих упражнений, вероятно, был поражен следующим обстоятельством: несмотря на то что доказанная формула имеет вид  $h = \pm n$ , где  $n$  — целое, которое можно найти (и тем самым вычислить  $h$ , поскольку  $h$ , по определению, положительно), фактически вычисления всегда дают *положительные* целые  $n$ , так что во всех указанных выше случаях  $h = n$ . Тот факт, что всегда получается знак «+», представляет собой один из аспектов задачи, к решению которой Гаусс приложил значительные усилия. В первом параграфе своей статьи [G4] по этому вопросу Гаусс пишет: «... задача будет решена, если найти этот знак. Однако изучение этого вопроса, который на первый взгляд кажется очень простым, ведет к совершенно неожиданным трудностям, и дальнейшие занятия в этом направлении, которые до сих пор не наталкивались ни на какие препятствия, настоятельно требуют других методов». Здесь не место обсуждать «другие методы» Гаусса; обобщенные Дирихле и многими другими, эти методы обра-

зуют очень важную главу в теории чисел<sup>1)</sup>. Данное упражнение посвящено изучению связи между проблемой знака в формуле числа классов и задачей нахождения знака, которой занимался Гаусс. В частности, Гаусс доказал, что для положительного целого  $n$  и  $r = e^{2\pi i/n}$  справедлива формула

$$1 + r + r^4 + r^9 + \dots + r^{(n-1)^2} = \begin{cases} (1+i)\sqrt{n} & \text{при } n \equiv 0 \pmod{4}, \\ \sqrt{n} & \text{при } n \equiv 1 \pmod{4}, \\ 0 & \text{при } n \equiv 2 \pmod{4}, \\ i\sqrt{n} & \text{при } n \equiv 3 \pmod{4}, \end{cases} \quad (5)$$

([G4], разд. 19). В каждом случае сравнительно просто найти *квадрат* обеих частей этой формулы (например, доказать, что при  $n \equiv 0 \pmod{4}$  квадрат суммы в левой части равен  $2in$ ), и задача сводится к доказательству того, что знак квадратного корня всегда совпадает со знаком, приведенным в формуле (4).

(а) Используя формулу (5), докажите, что формулу  $\theta_0 - \theta_1 = \pm\sqrt{\pm\lambda}$  из упр. 4 к § 4.5 (где  $D = \pm\lambda \equiv 1 \pmod{4}$ ,  $\lambda$  — простое) можно усилить и привести к виду  $\theta_0 - \theta_1 = \sqrt{\lambda}$ , если  $\lambda$  — простое,  $\lambda \equiv 1 \pmod{4}$ , и  $\theta_0 - \theta_1 = i\sqrt{\lambda}$ , если  $\lambda$  — простое,  $\lambda \equiv 3 \pmod{4}$ , при условии что в качестве  $\alpha$  выбирается *специальный* корень  $\lambda$ -й степени из единицы, равный  $e^{2\pi i/\lambda}$ .

(b) Основная формула, которую мы должны доказать, имеет вид  $m\bar{\mu} = \sqrt{m}$  при  $D > 0$  и  $m\bar{\mu} = i\sqrt{m}$  при  $D < 0$ . Иначе говоря,

$$\alpha + \binom{D}{2} \alpha^2 + \binom{D}{3} \alpha^3 + \dots + \binom{D}{m} \alpha^m = \begin{cases} \sqrt{m}, & \text{если } D > 0, \\ i\sqrt{m}, & \text{если } D < 0, \end{cases} \quad (6)$$

где  $D$  свободно от квадратов,  $m = |D|$ , если  $D \equiv 1 \pmod{4}$ ,  $m = 4|D|$ , если  $D \not\equiv 1 \pmod{4}$ , и  $\alpha = e^{2\pi i/m}$ . В случае простого  $m$  выведите эту формулу из (а).

(с) Докажите (6) при  $D = -1, -2, 2$ .

(d) При простом  $|D|$ ,  $D \equiv -1 \pmod{4}$ , выведите (6) из (b) и (с). [Сумму по всем  $s$  по модулю  $4p$  можно записать в виде суммы по всем  $s = 4a + pb$ , где  $a$  пробегает все целые по модулю  $p$ , а  $b$  пробегает все целые по модулю 4].

(е) При  $D = 2p$  ( $p$  — простое) выведите (6) из (b) и (с). [При  $p \equiv -1 \pmod{4}$  здесь применяется формула  $i^2 = -1$ .] Аналогичным образом докажите (6) при  $D = -2p$ .

(f) Наконец, используя рассуждения, аналогичные рассуждениям из (е), докажите, что если равенство (6) выполняется для некоторого данного значения  $D$  и если оно выполняется для простого  $m$ , то это равенство справедливо для  $Dp$ , где  $p$  — нечетное простое, не делящее  $D$ .

(g) Предположим, что  $D < 0$  и что формула Гаусса (5) известна (в действительности достаточно знать (5) для *простого*  $n$ ). Докажите, что тогда число классов равно  $-\left[\binom{D}{1} + \dots + \binom{D}{m} m\right]/m$ .

<sup>1)</sup> См. основополагающую статью Гаусса по этому вопросу и краткое изложение этой статьи в книге Смита [S3, разд. 20]. См. также совершенно иное доказательство Дирихле ([D6] или [D7], разд. 111-114). Очень интересное и простое доказательство, использующее контурное интегрирование, предложил Морделл [M1]. Почти каждая книга по высшей теории чисел содержит то или иное доказательство используемых здесь фактов. В качестве близкого к нам по времени источника с довольно полными ссылками можно использовать [W4].

(h) Предположим, что дана формула (5). Докажите, что при  $D < 0$  число классов задается формулами из приведенного ниже резюме.

(i) Если  $p$  — простое и  $p \equiv -1 \pmod{4}$ , то первая половина классов по модулю  $p$ , а именно  $1, 2, \dots, (p-1)/2$ , содержит больше квадратов, чем неквадратов по модулю  $p$ . Если  $p \equiv 1 \pmod{4}$ , то первая половина вычетов содержит равное число квадратов и неквадратов (а именно по  $(p-1)/4$  каждого), но первая четверть  $1, 2, \dots, (p-1)/4$  содержит больше квадратов, чем неквадратов. Докажите эти утверждения.

(j) Обратно, докажите, что из утверждения (i) следует равенство (5) при простых  $n$ . Таким образом, (i) и формула (5) при простых  $n$  равносильны.

## Резюме

Пусть  $P$  — положительное нечетное целое, свободное от квадратов и большее 1, а  $C_j$  — сумма  $\binom{s}{P} = \prod \binom{s}{p_i}$  (где  $P = p_1 p_2 \dots p_k$  — разложение  $P$  на простые множители) по всем  $s$ , удовлетворяющим неравенствам  $(j-1)/8 < s/P < j/8$  ( $j$ -й «октант»); тогда числа классов  $h$ , соответствующие следующим детерминантам  $D$ , равны:

если  $P \equiv 3 \pmod{4}$ ,  $D = -P$ , то  $h = (C_1 + C_2 + C_3 + C_4) / (2 - \binom{D}{2})$   
(за исключением случая, когда  $D = -3$ ,  $h = 1$ );

если  $P \equiv 1 \pmod{4}$ ,  $D = -P$ , то  $h = 2(C_1 + C_2)$ ;

если  $P \equiv 3 \pmod{4}$ ,  $D = -2P$ , то  $h = 2(C_2 + C_3)$ ;

если  $P \equiv 1 \pmod{4}$ ,  $D = -2P$ , то  $h = 2(C_1 - C_4)$ .

Если  $D = -1$  или  $-2$ , то  $h = 1$ . Как будет показано в следующем параграфе (упр. 3), при  $D \equiv 1 \pmod{4}$  знаменатель  $2 - \binom{D}{2}$  исчезает, если рассматривать порядок  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$  (как это делал Дирихле), а не полный порядок квадратичных целых детерминанта  $D$ .

## 9.6. Подпорядки

Формулы из § 9.2—9.4 позволяют найти числа элементов всех групп классов дивизоров из гл. 7, т. е. групп классов дивизоров, соответствующих полному порядку *всех* квадратичных целых для различных свободных от квадратов детерминантов  $D$ . В этом параграфе мы покажем, что для более общих групп классов дивизоров из гл. 8 число классов  $h$  отличается постоянным множителем от числа классов  $h_0$  полного порядка:  $h = th_0$ , причем множитель  $t$  легко вычислить.

Напомним, что для любого данного свободного от квадратов детерминанта  $D$  и для любого положительного целого <sup>1)</sup>  $t$  существует единственный подпорядок индекса  $t$  в порядке всех квадратичных целых детерминанта  $D$ . (Точнее, этот подпорядок совпадает с множеством  $\{x + yt\omega : x, y \text{ — целые}\}$ , где  $\omega = \sqrt{D}$  при  $D \not\equiv 1 \pmod{4}$  и  $\omega = (1 - \sqrt{D})/2$  при  $D \equiv 1 \pmod{4}$ ). Соответствующая группа

<sup>1)</sup> Это целое в гл. 8 мы обозначали через  $s$ . В данном параграфе  $s$  будет использоваться для обозначения переменной, стремящейся к 1.

классов дивизоров образована всеми дивизорами, взаимно простыми с  $t$ , причем дивизор  $A$  считается эквивалентным дивизору  $B$ , если  $A\bar{B}$  является дивизором некоторого целого из данного подпорядка. Пусть  $h$  — число таких классов эквивалентности, а  $h_0$  — число классов эквивалентности при  $t = 1$ . Мы собираемся показать, что  $h = mh_0$ , где  $m$  — легко вычисляемое целое.

Как подсказывает опыт, приобретенный при рассмотрении случаев, когда  $t = 1$ , формула для  $h$  получается с использованием равенства

$$\begin{aligned} h \lim_{s \downarrow 1} (s-1) \sum_{\substack{A \approx I \\ (N(A), t)=1 \\ N(A) > 0}} N(A)^{-s} &= \lim_{s \downarrow 1} (s-1) \sum_{\substack{(N(A), t)=1 \\ N(A) > 0}} N(A)^{-s} = \\ &= \lim_{s \downarrow 1} (s-1) \prod_{(N(P), t)=1} (1 - N(P)^{-s})^{-1}. \end{aligned}$$

Здесь запись  $A \approx B$  означает, что  $A\bar{B}$  является дивизором квадратичного целого из данного подпорядка ( $A \sim B$  будет означать, что  $A\bar{B}$  — дивизор квадратичного целого из полного порядка, так что  $A \approx B$  влечет за собой  $A \sim B$ ), а запись  $(N(A), t) = 1$  означает, что целые  $N(A)$  и  $t$  взаимно просты. Последнее из этих трех чисел можно также записать в виде

$$\begin{aligned} \lim_{s \downarrow 1} (s-1) \prod_{(N(P), t) \neq 1} (1 - N(P)^{-s}) \prod_P (1 - N(P)^{-s})^{-1} &= \\ &= \prod_{(N(P), t) \neq 1} (1 - N(P)^{-1}) \lim_{s \downarrow 1} (s-1) \sum_{N(A) > 0} N(A)^{-s} = \\ &= \prod_{(N(P), t) \neq 1} (1 - N(P)^{-1}) h_0 \lim_{s \downarrow 1} (s-1) \sum_{\substack{A \approx I \\ N(A) > 0}} N(A)^{-s}. \end{aligned}$$

Действительно, предел конечного произведения по простым дивизорам  $P$ , не взаимно простым с  $t$ , можно вычислять отдельно. Заметим, что из эквивалентности  $A \approx I$  следует эквивалентность  $A \sim I$ , поэтому сумма в левой части равенства

$$\begin{aligned} h \lim_{s \downarrow 1} (s-1) \sum_{\substack{A \approx I \\ (N(A), t)=1 \\ N(A) > 0}} N(A)^{-s} &= \\ &= h_0 \prod_{(N(P), t) \neq 1} (1 - N(P)^{-1}) \lim_{s \downarrow 1} (s-1) \sum_{\substack{A \approx I \\ N(A) > 0}} N(A)^{-s} \quad (1) \end{aligned}$$

получается из суммы в правой части вычеркиванием всех слагаемых, для которых  $A \not\approx I$  или  $(N(A), t) \neq 1$ . Поэтому задача, по существу, сводится к вычислению отношения этих сумм.

*Случай 1.*  $D < 0$ . Рассмотрим сначала случай, когда  $D$  не равно  $-1$  или  $-3$ , так что единственными единицами являются  $\pm 1$ .

Тогда каждый дивизор  $A$ , для которого  $A \sim I$ , является дивизором в точности двух квадратичных целых, а каждый дивизор  $A$ , для которого  $A \approx I$ , является дивизором в точности двух квадратичных целых, принадлежащих данному подпорядку. Таким образом, задача состоит в нахождении предела при  $s \downarrow 1$  отношения суммы  $\sum N(x + y\sqrt{D})^{-s}$  по всем квадратичным целым к сумме  $\sum N(x + y\sqrt{D})^{-s}$  только по тем квадратичным целым, которые принадлежат данному подпорядку и взаимно просты с  $t$ . Предположим, что точки  $xu$ -плоскости с целыми координатами поставлены в соответствие квадратичным целым посредством отображения  $(x, y) \leftrightarrow x + y\sqrt{D}$  для  $D \not\equiv 1 \pmod{4}$  и  $(x, y) \leftrightarrow x + y \cdot \frac{1}{2}(1 - \sqrt{D})$  для  $D \equiv 1 \pmod{4}$ . Разделим множество всех таких точек  $xu$ -плоскости на квадраты, каждая сторона которых содержит по  $t$  точек. Тогда каждый квадрат соответствует  $t^2$  слагаемым большей суммы и все эти  $t^2$  слагаемых являются величинами одного порядка. Ответ на вопросы о том, принадлежит ли  $x + y\omega$  ( $\omega = \sqrt{D}$  или  $\frac{1}{2}(1 - \sqrt{D})$ ) подпорядку индекса  $t$  и является ли это целое взаимно простым с  $t$ , зависит только от классов вычетов  $x$  и  $y$  по модулю  $t$ ; поэтому ясно, что число  $v$  из этих  $t^2$  слагаемых, соответствующих меньшей сумме, является одним и тем же для всех квадратов указанного разбиения. Действительно, каждый квадрат со стороной  $t$  содержит в точности  $t$  квадратичных целых из данного подпорядка ( $y$  фиксировано, а  $x$  пробегает  $t$  значений), среди которых  $\varphi(t)$  целых взаимно просты с  $t$ ; здесь  $\varphi(t)$  — число положительных целых, меньших  $t$  и взаимно простых с  $t$  (элемент  $x + y\omega$ , принадлежащий данному подпорядку, имеет вид  $x + vt\omega$  и взаимно прост с  $t$  тогда и только тогда, когда  $x$  взаимно просто с  $t$ ). Таким образом,  $v = \varphi(t)$ . Следующее утверждение интуитивно ясно, и его нетрудно доказать строго (упр. 5): поскольку каждый блок из  $t^2$  слагаемых большей суммы содержит  $\varphi(t)$  слагаемых меньшей суммы и все эти слагаемые являются величинами одного порядка, то при  $s \downarrow 1$  отношение большей суммы к меньшей стремится к отношению  $t^2$  к  $\varphi(t)$ . То есть

$$h = h_0 \prod_{(N(P), t) \neq 1} (1 - N(P)^{-1})^{\frac{t^2}{\varphi(t)}}.$$

Например, для квадратичных целых  $\{x + y\sqrt{-163} : x, y \text{ — целые}\}$  число классов  $h_0$  равно 1 (см. § 7.6),  $t = 2$ , существует в точности один простой дивизор, не взаимно простой с  $t$ , а именно простое 2 с нормой 4, и  $\varphi(t) = \varphi(2) = 1$ . Таким образом,

$$h = 1 \cdot \left(1 - \frac{1}{4}\right) \cdot \frac{2^2}{1} = 3,$$

как мы уже показали в § 8.5. Для квадратичных целых  $\{x + y\sqrt{-63} : x, y \text{ — целые}\}$  имеем  $D = -7$ ,  $t = 6$

$$h = 1 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{9}\right) \cdot \frac{6^2}{\varphi(6)} = \\ = \frac{1}{4} \cdot \frac{8}{9} \cdot \frac{36}{2} = 4.$$

Действительно, методами гл. 8 легко показать, что в этом случае 4 дивизора  $I, (11, 2), (11, 2)^2, (11, 2)^3$  образуют систему представителей группы классов дивизоров.

Эту формулу можно упростить дальше, используя известное и легко доказываемое соотношение:

$$\frac{\varphi(t)}{t} = \prod_{p|t} \left(1 - \frac{1}{p}\right)$$

(упр. 4). Поскольку

$$(1 - N(P)^{-1}) = \left(1 - \frac{1}{p}\right) \left(1 - \left(\frac{D}{p}\right) \frac{1}{p}\right),$$

это соотношение показывает, что в рассмотренном выше случае  $D < 0$ ,  $D \neq -1$ ,  $D \neq -3$  число классов равно

$$h = h_0 t \prod_{p|t} \left(1 - \left(\frac{D}{p}\right) \frac{1}{p}\right). \quad (2)$$

Если  $D = -1$ , то  $h$  равно половине заданного этой формулой числа. Действительно, в этом случае сумма значений  $N(A)^{-s}$  по всем главным дивизорам равна  $1/4$  суммы значений  $N(x + y\sqrt{D})^{-s}$  по всем ненулевым квадратичным целым, а не  $1/2$  этой суммы, тогда как сумма  $N(A)^{-s}$  по всем дивизорам  $A \approx I$ ,  $(N(A), t) = 1$ , по-прежнему равна  $1/2$  суммы по всем  $x + y\sqrt{D}$ , принадлежащим данному подпорядку и взаимно простым с  $t$  (поскольку подпорядок содержит в точности две единицы  $\pm 1$ : единицы  $\pm\sqrt{-1}$  не принадлежат ни одному собственному подпорядку). Аналогично, если  $D = -3$ , то  $h$  равно одной трети числа, заданного формулой (2).

Если  $D > 0$ , то, несколько видоизменяя проведенные выше рассуждения (упр. 6), легко показать, что

$$h = h_0 \cdot \frac{1}{k} \cdot t \prod_{p|t} \left(1 - \left(\frac{D}{p}\right) \frac{1}{p}\right), \quad (3)$$

где  $h_0$  — число классов полного порядка всех квадратичных целых детерминанта  $D$ ,  $h$  — число классов подпорядка индекса  $t$  и  $k$  — целое, определенное формулой  $E = E_0^k$ ; здесь  $E_0 = \varepsilon$  или  $\varepsilon^2$  — основная единица с нормой 1 в полном порядке и  $E$  — основная единица с нормой 1 в подпорядке индекса  $t$ .



Например, если  $D=5$  и  $t=2$ , то  $\varepsilon = \frac{1}{2}(1 + \sqrt{5})$ ,  $E_0 = \varepsilon^2 = \frac{1}{2}(3 + \sqrt{5})$ ,  $E_0^2 = \frac{1}{2}(7 + 3\sqrt{5})$ ,  $E_0^3 = 9 + 4\sqrt{5} = E$ . Следовательно,

$$h = 1 \cdot \frac{1}{3} \cdot 2 \left(1 + \frac{1}{2}\right) = 1.$$

Если  $D=11$ ,  $t=3$ , то  $\varepsilon = 10 + 3\sqrt{11} = E_0 = E$  и

$$h = h_0 \cdot \frac{1}{4} \cdot 3 \left(1 + \frac{1}{3}\right) = 4h_0.$$

Но  $h_0 = 2$ , следовательно,  $h = 8$ . Это можно проверить прямым вычислением (упр. 1).

## Упражнения

1. Найдите систему представителей группы классов дивизоров порядка  $\{x + y\sqrt{99} : x, y \text{ — целые}\}$ ; в частности, докажите, что число классов равно 8.

2. Найдите  $h$  для порядка  $\{x + y\sqrt{117} : x, y \text{ — целые}\}$  двумя способами: при помощи формулы (3); при помощи явного вычисления группы классов дивизоров.

3. Докажите, что знаменатель в первом случае формулы из упражнений к § 9.5 (см. резюме) исчезает, если рассматривать порядок  $\{x + y\sqrt{D} : x, y \text{ — целые}\}$ , а не полный порядок. Другими словами, если  $D$  отрицательно, свободно от квадратов и сравнимо с 1 по модулю 4, то число классов этого порядка равно количеству целых чисел  $n$  в множестве  $1, 2, \dots, \frac{1}{2}(|D|-1)$ , для которых  $\left(\frac{D}{n}\right) = +1$ , минус количество тех, для которых  $\left(\frac{D}{n}\right) = -1$ . Это утверждение впервые доказал Дирихле. При простом  $|D|$  Якоби высказал это утверждение в виде гипотезы. (Ссылки см. в [D7], § 104).

4. Докажите формулу

$$\frac{\varphi(t)}{t} = \prod_{p|t} \left(1 - \frac{1}{p}\right).$$

При простом  $t$  эта формула очевидна. Если  $t$  является степенью простого числа, то она почти столь же очевидна. Если  $t = uv$ , где  $u$  и  $v$  взаимно просты, то ее справедливость для  $t$  следует из ее справедливости для  $u$  и  $v$  (согласно китайской теореме об остатках). Этих замечаний достаточно для доказательства формулы.]

5. Докажите, что при  $s \downarrow 1$  отношение большей суммы к меньшей стремится к  $t^2/\varphi(t)$  (как и утверждалось в основном тексте). [Пусть  $\Sigma_0(s)$  — большая сумма и  $\Sigma_1(s)$  — меньшая сумма. Через  $\Sigma_2(s)$  обозначим сумму значений  $N(x + y\sqrt{D})^{-s}$  по центрам всех квадратов со стороной  $t$ , на которые разбиты квадратичные целые в доказательстве из основного текста. Докажите, что величины  $\Sigma_0(s) - t^2\Sigma_2(s)$  и  $\Sigma_1(s) - \varphi(t)\Sigma_2(s)$  остаются ограниченными при  $s \downarrow 1$ , а величина  $\Sigma_2(s)$  при  $s \downarrow 1$  не ограничена. Отсюда следует требуемое заключение.]

6. Докажите формулу (3). [Используйте метод записи суммы по всем главным дивизорам в виде суммы по некоторому подмножеству квадратичных целых (§ 9.3).]

### 9.7. Простые в арифметических прогрессиях

Было бы неразумно зайти так далеко в изучении работ Дирихле и не дать хотя бы наброска его знаменитой теоремы о простых в арифметических прогрессиях, несмотря на то, что эта теорема вообще не связана с Последней теоремой Ферма и не имеет практически никакого отношения к теории дивизоров квадратичных целых.

Согласно этой теореме, для любого целого  $a$  и любого целого  $b$ , взаимно простого с  $a$ , существует бесконечно много простых  $p$ , которые удовлетворяют сравнению  $p \equiv b \pmod{a}$ , т. е. лежат в арифметической прогрессии  $ax + b$  ( $x$  — целое). (Конечно, если  $b$  не взаимно просто с  $a$ , то сравнение  $p \equiv b \pmod{a}$  имеет не более одного решения.)

Доказательство этой теоремы начинается с обобщения формулы эйлерова произведения ( $\sum n^{-s} = \prod (1 - p^{-s})^{-1}$ ), которым мы уже пользовались в § 9.2, а именно с формулы

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p-\text{простые}} \frac{1}{1 - \frac{\chi(p)}{p^s}}. \quad (1)$$

Эта формула является формальным тождеством для любой функции  $\chi(n)$ , которая удовлетворяет соотношениям  $\chi(mn) = \chi(m)\chi(n)$ . (Разложите множители  $(1 - \chi(p)p^{-s})^{-1}$  в правой части в бесконечные ряды и формально перемножьте их.) Если  $\chi$  — такая ограниченная функция, переводящая положительные целые числа в вещественные или даже комплексные, то обе части (1) сходятся при  $s > 1$ , и формула (1) справедлива (не только формально).

Рассмотренные выше функции  $\chi(n) = \left(\frac{D}{n}\right)$  представляют собой только частный случай функций  $\chi$ , удовлетворяющих двум условиям:  $\chi(mn) = \chi(m)\chi(n)$  и  $\chi$  ограничена. При изучении простых в арифметических прогрессиях естественно подчинить такие функции  $\chi$  двум дополнительным условиям:  $\chi(n+a) = \chi(n)$  при всех  $n$  и  $\chi(n) = 0$  при  $n$ , не взаимно простых с  $a$ . Не равная тождественно нулю функция  $\chi$ , которая удовлетворяет всем этим условиям, называется *характером* по модулю  $a$ . Нахождение всех таких характеров  $\chi$  для данного  $a$  представляет собой простое упражнение. Например, при  $a = 20$  все характеры  $\chi$  можно найти следующим образом. Поскольку  $\chi(n) = \chi(1 \cdot n) = \chi(1) \cdot \chi(n)$  для всех  $n$ , то из  $\chi(1) \neq 1$  следовало бы, что  $\chi(n) = 0$  для всех  $n$ . Следовательно,  $\chi(1) = 1$ . Все значения  $\chi$  будут известны, если найти  $\chi(3)$ ,  $\chi(7)$ ,  $\chi(9)$ ,  $\chi(11)$ ,  $\chi(13)$ ,  $\chi(17)$  и  $\chi(19)$ . Так как  $19^2 \equiv (-1)^2 \equiv 1 \pmod{20}$ , то  $\chi(19)^2 = \chi(19^2) = \chi(1) = 1$ . Следовательно,  $\chi(19) = \pm 1$ . Если известно  $\chi(19)$ , то достаточно

найти  $\chi(3)$ ,  $\chi(7)$  и  $\chi(9)$ . Действительно,  $\chi(11) = \chi(-9) = \chi(19)\chi(9)$ ,  $\chi(13) = \chi(19)\chi(7)$  и  $\chi(17) = \chi(19)\chi(3)$ . Ясно, что  $\chi(9) = \pm 1$ . Кроме того,  $\chi(9) = \chi(3)^2$ . Следовательно,  $\chi(3) = 1, -1, i$  или  $-i$ . Если известно  $\chi(3)$ , то можно найти не только  $\chi(9) = \chi(3)^2$ , но и  $\chi(7) = \chi(3)^3$ . Это показывает, что  $\chi(3)$  принимает одно из четырех значений, а  $\chi(19)$  принимает одно из двух значений, и этих двух значений  $\chi(3)$  и  $\chi(19)$  достаточно для нахождения всех остальных. Легко проверить (см. упр. 2), что все  $4 \times 2 = 8$  возможных выборов  $\chi(3)$  и  $\chi(19)$  приводят к характерам. Следовательно, восемь характеров  $\chi$ , приведенных в табл. 9.7.1, дают все характеры по модулю 20.

Таблица 9.7.1.

	$\chi(1)$	$\chi(3)$	$\chi(7)$	$\chi(9)$	$\chi(11)$	$\chi(13)$	$\chi(17)$	$\chi(19)$
$\chi_0$	1	1	1	1	1	1	1	1
$\chi_1$	1	$i$	$-i$	-1	-1	$-i$	$i$	1
$\chi_2$	1	-1	-1	1	1	-1	-1	1
$\chi_3$	1	$-i$	$i$	-1	-1	$i$	$-i$	1
$\chi_4$	1	1	1	1	-1	-1	-1	-1
$\chi_5$	1	$i$	$-i$	-1	1	$i$	$-i$	-1
$\chi_6$	1	-1	-1	1	-1	1	1	-1
$\chi_7$	1	$-i$	$i$	-1	1	$-i$	$i$	-1

Характер, определенный условием « $\chi(n) = 1$  при  $n$ , взаимно простом с  $a$ », называется *главным характером* по модулю  $a$  и обозначается  $\chi_0$ . Для этого характера функция (1) имеет вид

$$\prod_{p \nmid a} \frac{1}{1 - p^{-s}} = \prod_{p|a} (1 - p^{-s}) \zeta(s).$$

В частности, при  $s \downarrow 1$  эта функция стремится к  $+\infty$ , поскольку  $\zeta(s)$  стремится к  $+\infty$ , а конечное произведение в правой части стремится к положительной постоянной. (В § 9.6 было показано, что эта постоянная равна  $\varphi(a)/a$ .)

Обозначим через  $L(s, \chi)$  функцию, определенную формулой (1) при  $s > 1$  (для введенных выше характеров  $\chi$ ). Мы только что доказали, что  $\lim_{s \downarrow 1} L(s, \chi_0) = +\infty$ . В противоположность этому, если  $\chi$  — произвольный характер по модулю  $a$ , *отличный* от главного характера  $\chi_0$ , то предел  $L(s, \chi)$  не только не является бесконечным, но и ряд в левой части (1) условно сходится при  $s > 0$  и при этих значениях  $s$  определяет непрерывную функцию от  $s$ . Если доказать, что  $\sum_{j=1}^a \chi(j) = 0$ , то, используя суммирование по частям (так же, как и в § 6.5), можно доказать

эти утверждения о сходимости. Равенство  $\sum_{j=1}^a \chi(j) = 0$  получается из тождества

$$\chi(k) \sum_{j=1}^a \chi(j) = \sum_{j=1}^a \chi(kj) = \sum_{j'=1}^a \chi(j')$$

( $k$  взаимно просто с  $a$ ), которое показывает, что если  $\sum \chi(j) \neq 0$ , то  $\chi(k) = 1$  для всех  $k$ , взаимно простых с  $a$ .

Таким образом, существует конечный набор таких функций  $L(s, \chi)$ , одна из которых при  $s \downarrow 1$  стремится к  $\infty$ , а остальные стремятся к конечным пределам.

Рассмотрим теперь логарифмы этих функций. Используя разложения из правой части (1), получим при  $s > 1$

$$\begin{aligned} \log L(s, \chi) &= \sum_p \log \frac{1}{1 - \chi(p) p^{-s}} = \sum_p \left[ \sum_m \frac{1}{m} (\chi(p) p^{-s})^m \right] = \\ &= \sum_q \sum_m \frac{1}{m} \chi(p^m) p^{-ms}; \end{aligned}$$

здесь мнимая часть  $\log L(s, \chi)$  определена так, чтобы выполнялось это равенство. Слагаемые этого ряда, для которых  $m \geq 2$ , сходятся при  $s > 1/2$  и стремятся к конечному пределу при  $s \downarrow 1$ . Следовательно, если не обращать внимания на такие слагаемые, мы получим

$$\log L(s, \chi) \sim \sum_p \frac{\chi(p)}{p^s}, \quad (2)$$

где символ  $\sim$  означает, что разность между обеими частями остается ограниченной при  $s \downarrow 1$ .

Для доказательства теоремы Дирихле достаточно показать, что

$$\lim_{s \downarrow 1} \sum_{p \equiv b \pmod{a}} \frac{1}{p^s} \quad (3)$$

бесконечен. Действительно, если бы этот ряд содержал только конечное число слагаемых, то его предел был бы равен конечной сумме  $\sum (1/p)$ . Но сумма в правой части (3) при каждом  $b$ , взаимно простом с  $a$ , представляет собой комбинацию сумм из правой части (2). Например, если  $a = 20$  и  $b = 7$ , то функция  $\chi_0 + i\chi_1 - \chi_2 - i\chi_3 + \chi_4 + i\chi_5 - \chi_6 - i\chi_7$  удовлетворяет соотношениям  $f(n+20) = f(n)$ ,  $f(n) = 0$  при  $n$ , не взаимно простом с 20,  $f(7) = 8$  и легко проверить, что  $f(1) = f(3) = f(9) = f(11) = f(13) = f(17) = f(19) = 0$ . Вообще, нетрудно доказать, что при любом  $k$ , взаимно простом с 20,  $\sum \chi_j(k)^{-1} \chi_j = f$  обладает свойствами:  $f(k) = 8$ ,  $f(j) = 0$  при  $j \not\equiv k \pmod{20}$  (упр. 7).

Следовательно,

$$\begin{aligned} \sum_{p \equiv 7 \pmod{20}}^8 \frac{1}{p^s} &= \sum_p \left[ \sum_{v=1}^8 \chi_v(7)^{-1} \chi_v(p) \right] \frac{1}{p^s} = \\ &= \sum_{v=1}^8 \chi_v(7)^{-1} \left[ \sum_p \frac{\chi_v(p)}{p^s} \right] \sim \\ &\sim \sum_{v=1}^8 \chi_v(7)^{-1} \log L(s, \chi_v), \end{aligned}$$

где символ  $\sim$  снова означает, что разность обеих частей остается ограниченной при  $s \downarrow 1$ .

Функция  $\log L(s, \chi_0)$  принимает вещественные значения и стремится к  $\infty$  при  $s \downarrow 1$ . Поэтому для доказательства того, что предел выражения (3) (при  $a = 20, b = 7$ ) при  $s \downarrow 1$  равен  $\infty$ , достаточно доказать, что для  $v \neq 0$  функция  $\operatorname{Re} \log L(s, \chi_v)$  остается ограниченной при  $s \downarrow 1$ , т. е. что  $\operatorname{Re} \log L(s, \chi_v) \sim 0$  при  $v \neq 0$ . Но  $L(s, \chi_v)$  стремится к  $L(1, \chi_v)$  при  $s \downarrow 1$ , следовательно, достаточно доказать, что  $L(1, \chi_v) \neq 0$ . Действительно, функция  $\operatorname{Re} \log$  непрерывна и определена для всех ненулевых комплексных чисел, поэтому из  $L(1, \chi_v) \neq 0$  следует, что  $\operatorname{Re} \log L(s, \chi_v)$  стремится к конечному пределу  $\operatorname{Re} \log L(1, \chi_v)$  при  $s \downarrow 1$  и, в частности, ограничена.

Точно так же можно доказать, что

$$\varphi(a) \sum_{p \equiv b \pmod{a}} \frac{1}{p^s} \sim \sum_{\chi} \chi(b)^{-1} \log L(s, \chi),$$

где  $\varphi(a)$  — число характеров (можно показать, что оно равно количеству целых, меньших  $a$  и взаимно простых с  $a$ ) и где суммирование в правой части производится по всем  $\varphi(a)$  характерам. Если доказать, что  $L(1, \chi) \neq 0$  при  $\chi \neq \chi_0$ , то мы получим, что

$$\operatorname{Re} \log L(s, \chi) \sim 0$$

при  $\chi \neq \chi_0$  и, следовательно,

$$\sum_{p \equiv b \pmod{a}} \frac{1}{p^s} \sim \frac{1}{\varphi(a)} \log L(s, \chi_0)$$

(поскольку  $\chi_0(b) = 1$ ). При этом будет доказано не только то, что существует бесконечно много простых в арифметической прогрессии  $ax + b$ , но и что простые довольно равномерно распределены по всем  $\varphi(a)$  возможным прогрессиям (в том смысле, что разность между суммами (3) для двух различных значений  $b$  остается ограниченной при  $s \downarrow 1$ ). Действительно, эти разности на

ограниченные величины отличаются от  $\varphi(a)^{-1} \log L(s, \chi_0) \sim \sim \varphi(a)^{-1} \log \zeta(s) \sim -\varphi(a)^{-1} \log(s-1)$ .

Короче говоря, для доказательства теоремы Дирихле достаточно доказать, что  $L(1, \chi) \neq 0$  при любом неглавном характере  $\chi$  по модулю  $a$ . При  $a = 20$  это можно сделать следующим образом. Суммируя (2) по всем  $\varphi(a)$  характерам, получим:

$$\sum \log L(s, \chi) \sim \sum_{p \equiv 1 \pmod{a}} p^{-s}.$$

Вещественнозначная сумма в правой части при  $s \downarrow 1$  ограничена снизу (в действительности она неотрицательна). Следовательно,  $\prod L(s, \chi)$  отделено от нуля при  $s \downarrow 1$ . Как и в § 6.7, отсюда следует, что *самое большее одна* из функций  $L(s, \chi)$  может обращаться в нуль при  $s = 1$  ( $L(s, \chi_0) (s-1)$  остается ограниченной при  $s \downarrow 1$ ) и, следовательно,  $L(1, \bar{\chi})$  не может обращаться в нуль, если  $\chi \neq \bar{\chi}$ . Таким образом, достаточно доказать, что  $L(1, \chi) \neq 0$  для *вещественных* неглавных характеров  $\chi$ , т. е. для характеров  $\chi_2, \chi_4, \chi_6$  в рассматриваемом примере.

Формула числа классов из § 9.2 при  $D = -5$  показывает, что  $L(1, \chi_4) \neq 0$  (поскольку  $\chi_4$  совпадает с характером из этой формулы). Из формулы числа классов при  $D = 5$  следует, что число

$$\begin{aligned} 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \dots = \\ = \prod_p \frac{1}{1 - \binom{D}{p} \frac{1}{p}} = \frac{1}{1 - \binom{D}{2} \frac{1}{2}} \prod_{p \neq 2} \frac{1}{1 - \binom{D}{p} \frac{1}{p}} = \frac{2}{3} L(1, \chi_2) \end{aligned}$$

отлично от нуля ( $\chi_2(n)$  равно нулю для четных  $n$  и совпадает с  $\binom{D}{n}$  для нечетных  $n$ ; здесь  $D = 5$ ). Следовательно,  $L(1, \chi_2) \neq 0$ . Наконец,  $\chi_6(p) = \binom{-1}{p}$  (за исключением  $\chi_6(5) = 0$  и  $\binom{-1}{5} = 1$ ). Следовательно,

$$\begin{aligned} L(1, \chi_6) &= \prod_p \frac{1}{1 - \chi_6(p) p^{-1}} = \left(1 - \binom{-1}{5} 5^{-1}\right) \prod_p \frac{1}{1 - \binom{-1}{p} \frac{1}{p}} = \\ &= \frac{4}{5} \left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots\right) = \frac{\pi}{5} \neq 0. \end{aligned}$$

Это и доказывает, что

$$\sum_{p \equiv b \pmod{20}} \frac{1}{p^s} \sim \frac{1}{8} \log(s-1)$$

для всех 8 возможных значений  $b$  по модулю 20.

В общем случае доказательство того, что вещественный характер  $\chi$  по модулю  $a$  совпадает (с точностью до нескольких простых)



с характером  $\left(\frac{D}{n}\right)$  из формулы числа классов, представляет собой довольно простую алгебраическую задачу. Поскольку число классов отлично от нуля, мы получаем отсюда, что  $L(1, \chi) \neq 0$  для всех таких  $\chi$  и, как было показано выше,

$$\sum_{p \equiv b \pmod{a}} \frac{1}{p^s} \sim \frac{1}{\varphi(a)} \log \frac{1}{s-1}$$

при всех  $\varphi(a)$  возможных значениях  $b$  по модулю  $a$ . Здесь символ  $\sim$  означает, что разность обеих частей остается ограниченной при  $s \downarrow 1$ . В частности, число слагаемых в левой части бесконечно, и отсюда следует теорема Дирихле.

## Упражнения

1. Пусть  $n$  взаимно просто с  $a$ . Докажите, что существует такое положительное целое  $j$ , что  $n^j \equiv 1 \pmod{a}$ . Докажите, что ненулевые значения характеров по модулю  $a$  должны быть корнями  $\varphi(a)$ -й степени из единицы.

2. Пусть  $a = \alpha\beta$ , где  $\alpha$  и  $\beta$  — взаимно простые целые. Докажите, что любой характер по модулю  $a$  можно единственным образом представить в виде произведения характера по модулю  $\alpha$  и характера по модулю  $\beta$ . Кроме того, произведение будет вещественным тогда и только тогда, когда вещественны сомножители. Это показывает, что для нахождения всех характеров или всех вещественных характеров по модулю  $a$  достаточно решить соответствующую задачу для  $a$ , являющихся степенями простого числа. [Определите  $\chi_\alpha$  условием  $\chi_\alpha(k) = \chi(s)$  при  $s \equiv k \pmod{\alpha}$  и  $s \equiv 1 \pmod{\beta}$ .]

3. Предположим, что  $a = p^m$ , где  $p$  — простое число, отличное от 2. Докажите, что существуют  $\varphi(a) = a(p-1)/p$  характеров по модулю  $a$ . Среди них в точности два (еще один характер, кроме главного) являются вещественнозначными. Кроме главного таким характером является символ Лежандра  $\chi(n) = \left(\frac{n}{p}\right)$ . Используя формулу числа классов, докажите для этого  $\chi$ , что  $L(1, \chi) \neq 0$ . [Если  $m = 1$ , то через  $\gamma$  обозначим примитивный корень по модулю  $p$ . Тогда  $\chi$  полностью определяется значением  $\chi(\gamma)$  и  $\chi$  будет вещественным характером, только если  $\chi(\gamma) = \pm 1$ . Следовательно, в этом случае найти доказательство легко. Легко разобраться и в случае  $m > 1$ , если доказать, что существует такое целое, степени которого по модулю  $p^m$  содержат все  $(p-1)p^{m-1}$  классов по модулю  $p^m$ , взаимно простых с  $p^m$ . Рассмотрим теперь случай  $m = 2$ . Пусть  $\gamma$  — примитивный корень по модулю  $p$ . Тогда  $\gamma$  является примитивным корнем по модулю  $p^2$  в том и только в том случае, когда  $\gamma^{p-1} \not\equiv 1 \pmod{p^2}$ . Действительно, наименьшая степень  $\gamma$ , сравнимая с 1 по модулю  $p^2$ , должна делить  $\varphi(p^2) = (p-1)p$ . Если  $\gamma$  — произвольный примитивный корень по модулю  $p$  и  $\gamma^{p-1} \equiv 1 \pmod{p^2}$ , то  $(\gamma + p)^{p-1} \equiv 1 \pmod{p^2}$ . Следовательно, всегда существует примитивный корень по модулю  $p^2$  (даже при  $p = 2$ ). Для такого примитивного корня  $\gamma^{p-1} = 1 + hp$ , где  $h \not\equiv 0 \pmod{p}$ . Тогда, если  $p \neq 2$ , то  $\gamma^{(p-1)p} \equiv 1 + hp^2 \pmod{p^3}$ . Отсюда следует, что  $\gamma$  является примитивным корнем по модулю  $p^3$  и  $\gamma^{(p-1)p} \equiv 1 + hp^3 \pmod{p^4}$ . Продолжение этого процесса показывает, что  $\gamma$  является примитивным корнем по модулю  $p^m$  для всех  $m \geq 2$  тогда и только тогда, когда  $\gamma$  — примитивный корень по модулю  $p^2$ . Следовательно, для всех  $m$  существуют примитивные корни по модулю  $p^m$ .]

4. Если  $a = 2$ , то имеется только главный характер. При  $a = 4$  есть два характера: главный характер и  $\chi(n) = \left(\frac{-1}{n}\right)$ . Если  $a = 2^m$  при  $m > 2$ , то существуют  $2^{m-1}$  характеров, среди которых 4 характера вещественны, а именно главный характер и характеры  $\chi(n) = \left(\frac{-1}{n}\right)$ ,  $\chi(n) = \left(\frac{2}{n}\right)$ ,  $\chi(n) = \left(\frac{-2}{n}\right)$ . Докажите, что для каждого из 3 неглавных вещественных характеров  $\chi$  число  $L(1, \chi) \neq 0$ . [Сравнения  $5 \equiv 1 + 4 \pmod{8}$ ,  $5^2 \equiv 1 + 8 \pmod{16}$ ,  $5^4 \equiv 1 + 16 \pmod{32}$ ,  $5^8 \equiv 1 + 32 \pmod{64}$ ,  $5^{16} \equiv 1 + 64 \pmod{128}$ , ... показывают, что порядок числа 5 по модулю  $2^m$ , т. е. наименьшая степень числа 5, сравнимая с 1 по модулю  $2^m$ , не делится на  $2^{m-3}$ . Таким образом, порядок числа 5 равен  $2^{m-2}$  или  $2^{m-1}$ . Если бы его порядок был  $2^{m-1}$ , то любое нечетное целое совпадало бы с некоторой степенью числа 5 по модулю  $2^m$ . Но это невозможно, поскольку 3 не равно никакой степени 5 по модулю 8. Покажите, что каждое целое сравнимо точно с одним из целых вида  $3^\varepsilon 5^j$ , где  $\varepsilon = 0$  или 1 и  $j = 0, 1, 2, \dots, 2^{m-2} - 1$ . Это дает  $2^{m-1}$  характеров, среди которых 4 характера вещественны.]

5. Покажите, что число вещественных характеров по модулю  $a$  можно найти следующим образом. Пусть  $a = 2^\mu a'$ , где  $a'$  нечетно и делится на  $v$  различных простых. Если  $\mu = 0$  или 1, то число вещественных характеров равно  $2^v$ ; при  $\mu = 2$  это число равно  $2 \cdot 2^v$ ; если же  $\mu \geq 3$ , то число таких характеров равно  $4 \cdot 2^v$ .

6. Покажите, что для каждого вещественного характера из упр. 5 существует такое целое число  $D$ , что этот характер совпадает с  $\chi_D(n) = \left(\frac{D}{n}\right)$  с точностью до конечного множества простых  $p$ , для которых этот характер равен нулю на всех кратных  $p$ , а  $\chi_D$  отличен от нуля. Выведите отсюда, что  $L(1, \chi)$  отличается от  $L(1, \chi_D)$  на конечное число ненулевых множителей. Согласно формуле для числа классов,  $L(1, \chi_D) \neq 0$ , следовательно,  $L(1, \chi) \neq 0$  для всех вещественных неглавных характеров  $\chi$  по модулю  $a$ .

7. Предположим, что  $k$  взаимно просто с  $a$ . Докажите, что сумма значений  $\chi(k)^{-1} \chi(j)$  по всем характерам  $\chi$  равна 0, если  $j \not\equiv k \pmod{a}$ . (Конечно, при  $j \equiv k \pmod{a}$  эта сумма равна  $\phi(a)$ .) [Достаточно доказать, что сумма значений  $\chi(j)$  по всем характерам  $\chi$  равна нулю при  $j \not\equiv 1 \pmod{a}$ . Произведение двух характеров снова является характером, поэтому сумма  $\chi(j)$  по всем  $\chi$  совпадает с суммой  $\chi'(j) \chi(j)$  по всем  $\chi$  при любом фиксированном характере  $\chi'$ . Если эта сумма отлична от нуля, то  $\chi'(j)$  должно быть равно 1 для всех характеров  $\chi'$ . Поэтому достаточно доказать, что при  $j \not\equiv 1 \pmod{a}$  существует такой характер  $\chi'$  по модулю  $a$ , для которого  $\chi'(j) \neq 1$ . Согласно упр. 2, достаточно доказать это утверждение в случае, когда  $a$  является степенью простого числа. Если  $a = p^m$  и  $p \neq 2$ , то определим  $\chi'$  условием  $\chi'(\gamma) = e^{2\pi i / \phi(a)}$ , где  $\gamma$  — примитивный корень по модулю  $a$ . Тогда  $\chi'(j) = 1$  только при  $j \equiv 1 \pmod{a}$ . Пусть  $a = 2^m$ . Если  $m \geq 3$  и  $j \equiv 1 \pmod{8}$ , то характер  $\chi'$ , определенный условиями  $\chi'(3) = 1$ ,  $\chi'(5) = e^{2\pi i / \sigma}$ ,  $\sigma = 2^{m-2}$ , обладает свойством  $\chi'(j) \neq 1$ . В противном случае для одного из *вещественных* характеров  $\chi'$  выполняется свойство  $\chi'(j) \neq 1$  при  $j \not\equiv 1 \pmod{a}$ .]

## Приложение

### НАТУРАЛЬНЫЕ ЧИСЛА

#### А.1. Основные свойства

Теория чисел — это в первую очередь и главным образом изучение свойств *натуральных чисел*, т. е. чисел  $1, 2, 3, \dots$ , встречающихся в процессе *счета*. Именно процесс счета — например, сколько раз осуществилась некоторая повторяющаяся операция, — вот что придает натуральным числам их значение и что лежит в основе соотношений между ними. Говорят, что  $k = m + n$ , если осуществление операции  $m$  раз, а затем ее осуществление еще  $n$  раз сводится к осуществлению ее  $k$  раз подряд. Говорят, что  $k = mn$ , если  $m$  повторений серии, состоящей из осуществления операции  $n$  раз, сводится к осуществлению этой операции  $k$  раз подряд. Говорят, что  $k < m$ , если осуществление операции  $k$  раз приводит к тому, что операция осуществлена меньше чем  $m$  раз.

Основные факты, относящиеся к натуральным числам, включают в себя следующее. Сказать, что  $k < m$ , — это то же самое, что сказать, что имеется натуральное число  $n$ , для которого  $m = k + n$ . Если  $k < m$ , то  $k + n < m + n$  для всех  $n$ , и обратно, если  $k + n < m + n$  для некоторого  $n$ , то  $k < m$ . Аналогично,  $k < m$  тогда и только тогда, когда  $kn < mn$ . Если  $k < m$  и  $m < n$ , то  $k < n$ . Для любых  $k$  и  $m$  выполняется точно одно из трех отношений  $k < m$ ,  $k = m$ ,  $k > m$ . Действия сложения и умножения ассоциативны и коммутативны, и умножение дистрибутивно относительно сложения:

$$(k + m) + n = k + (m + n), \quad (km)n = k(mn),$$

$$k + m = m + k, \quad km = mk,$$

$$k(m + n) = km + kn.$$

Суммы и произведения можно *сокращать*, т. е. если  $k + n = m + n$ , то  $k = m$ , и если  $kn = mn$ , то  $k = m$ . (Тот факт, что можно сокращать произведения, делает натуральные числа более простыми в обращении, чем целые. Ведь при работе с целыми числами мы должны постоянно напоминать себе, что закон сокращения произведений выполняется для них только с дополнительной оговоркой  $n \neq 0$ .) Число  $1$  есть наименьшее натуральное число. Число  $n + 1$  есть наименьшее число из чисел, больших  $n$ . Оно

следует за числом  $n$ . Если  $n > 1$ , то  $n = 1 + m$  для некоторого  $m$ . При этом число  $m$  меньше  $n$  и является наибольшим среди чисел, меньших  $n$ . Оно предшествует числу  $n$ . Число 1 является единицей по умножению, т. е.  $1 \cdot n = n$ .

Принцип бесконечного спуска устанавливает, что убывающая последовательность натуральных чисел должна закончиться. Этот принцип может быть положен в основу большинства доказательств, относящихся к натуральным числам. Рассмотрим, например, основные факты, касающиеся деления. Если  $k$  и  $m$  — натуральные числа, причем  $k \leq m$ , то либо  $k$  делит  $m$ , т. е. имеется такое натуральное число  $q$ , что  $m = qk$ , либо однозначно определены такие натуральные числа  $q$  и  $r$ , что  $m = qk + r$  и  $r < k$ . Для доказательства сначала заметим, что 1 делит любое натуральное число, и поэтому можно предположить, что  $k > 1$ . Тогда  $mk > m$ . Поскольку  $m \geq k > 1$ , для числа  $m$  имеется предшествующее; обозначим его  $m - 1$ . Оно может удовлетворять или не удовлетворять условию  $(m - 1)k > m$ . Если оно ему удовлетворяет, для него имеется предшествующее число, которое мы обозначим  $m - 2$ . Тогда условие  $(m - 2)k > m$  может выполняться или не выполняться. Повторение этого процесса привело бы к бесконечно убывающей последовательности чисел, если бы на некотором этапе мы не получили бы число  $n$  (предшествующее предшествующему... числу  $m$ ), для которого  $nk$  не больше  $m$ , но  $(n + 1)k > m$ . Таким образом, на основании принципа бесконечного спуска, такое целое число  $n$  найдется. Тогда либо  $nk = m$ , либо  $nk < m$ . Если  $nk = m$ , то  $k$  делит  $m$  и первая альтернатива установлена. Если  $nk < m$ , то  $m = nk + r$  для некоторого  $r$ . Так как  $(n + 1)k > m$ ,  $nk + k > nk + r$ , то отсюда следует, что  $k > r$ . Наконец, если  $m = qk + s$ , где  $s < k$ , то  $q = n$ , ибо иначе  $q < n$  или  $q > n$ ; если  $q > n$ , то  $q = n + a$  для некоторого  $a$ ,  $nk + r = m = qk + s = nk + ak + s$ ,  $r = ak + s > k$ , вопреки предположению, и таким же способом приводится к противоречию случай  $n > q$ . Таким образом,  $q = n$  и  $qk + r = m = qk + s$ , откуда следует, что  $r = s$  и предложение доказано.

Наиболее важной конструкцией для натуральных чисел, выходящей за рамки этих элементарных арифметических фактов, является, по-видимому, алгоритм Евклида<sup>1)</sup> для нахождения наибольшего общего делителя двух натуральных чисел. Этот алгоритм, который можно охарактеризовать фразой «измеряй большее меньшим», представляет собой следующую процедуру. Пусть  $k$ ,  $m$  — данные натуральные числа, и предположим, не ограничивая общности, что  $k \leq m$ . Тогда либо  $k$  делит («измеряет»)  $m$ , либо  $m = qk + r$ , где  $r < k$ . В последнем случае положим  $m' = k$ ,  $k' = r$  и повторим процедуру (измерим большее мень-

<sup>1)</sup> «Начала» Кн. VII, предложения 1 и 2.

шим), найдя, что либо  $k'$  делит  $m'$ , либо  $m' = q'k' + r'$ , где  $r' < k'$ . В последнем случае положим  $m'' = k'$ ,  $k'' = r'$  и снова все повторим. Продолжаем, пока не наступит момент, когда деление произойдет без остатка. Иными словами, положим  $a_0 = m$ ,  $a_1 = k$  и определим последовательность  $a_0 > a_1 > a_2 > \dots > a_n$  условиями

$$\begin{array}{ll} a_0 = q_1 a_1 + a_2 & a_1 > a_2 \\ a_1 = q_2 a_2 + a_3 & a_2 > a_3 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ a_{n-2} = q_{n-1} a_{n-1} + a_n & a_{n-1} > a_n \\ a_{n-1} = q_n a_n. & \end{array}$$

Из принципа бесконечного спуска следует, что должен наступить такой момент, когда деление выполнится без остатка, поскольку иначе последовательность  $a_0 > a_1 > a_2 > \dots$  убывала бы бесконечно. Число  $a_n$  тогда является наибольшим общим делителем (или «наибольшей общей мерой») двух данных чисел  $a_0, a_1$ . Это означает, что  $a_n$  делит как  $a_0$ , так и  $a_1$  (последнее равенство показывает, что  $a_n$  делит  $a_{n-1}$ , затем предпоследнее равенство показывает, что  $a_n$  делит  $a_{n-2}$ , и дальнейший подъем по списку равенств показывает, что  $a_n$  делит все  $a_i$ ) и что любое число, делящее как  $a_0$ , так и  $a_1$ , делит и  $a_n$  (первое равенство показывает, что такое число должно делить  $a_2$ , затем второе равенство показывает, что оно должно делить  $a_3$ , и т. д., пока не дойдем до предпоследнего равенства, которое показывает, что это число должно делить  $a_n$ ). Таким образом, алгоритм Евклида не только доказывает существование наибольшего общего делителя двух чисел, но и дает явный способ его *нахождения* путем последовательных делений.

Два натуральных числа  $a$  и  $b$  называются *сравнимыми* по модулю третьего натурального числа  $c$ , что записывается  $a \equiv b \pmod{c}$ , если имеются такие натуральные числа  $m$  и  $n$ , что  $a + mc = b + nc$ . Другими способами выразить то же самое можно, сказав, что  $a$  и  $b$  лежат в одной и той же арифметической прогрессии с разностью  $c$ , или что  $a$  и  $b$  дают одинаковый остаток при делении на  $c$ . Легко видеть, что отношение сравнимости обладает следующими свойствами. Сравнимость по модулю  $c$  является *отношением эквивалентности*, т. е. она рефлексивна ( $a \equiv a \pmod{c}$  для любого  $a$ ), симметрична ( $a \equiv b \pmod{c}$  в том и только том случае, когда  $b \equiv a \pmod{c}$ ), и транзитивна (если  $a \equiv b \pmod{c}$  и  $b \equiv d \pmod{c}$ , то  $a \equiv d \pmod{c}$ ). Она согласована как со сложением, так и с умножением чисел. Это означает, что если  $a \equiv b \pmod{c}$ , то  $a + d \equiv b + d \pmod{c}$  для любого  $d$  и  $ad \equiv bd \pmod{c}$  для любого  $d$ . Таким образом, классы сравнений по модулю  $c$  можно складывать и перемножать очевидным образом: чтобы сложить (перемножить) два класса, нужно в каждом выб-



рать по числу и сложить (перемножить) их. Класс результата не зависит от этого выбора (если  $a \equiv a'$  и  $b \equiv b'$ , то  $a + b \equiv a + b' \equiv a' + b'$  и  $ab \equiv ab' \equiv a'b'$ ), и, следовательно, мы вправе назвать этот класс суммой (произведением) двух данных классов. При сложении классов сравнений выполняется значительно более сильное свойство, чем свойство сокращения, а именно: для любых заданных  $a, b, c$  имеется такое число  $x$ , что  $a + x \equiv b \pmod{c}$  и любые два решения  $x$  этой задачи сравнимы по модулю  $c$ . Действительно,  $b + nc > a$  для достаточно большого  $n$  (скажем,  $n = a$ ), так что  $b + nc = a + x$ , откуда вытекает сравнение  $a + x \equiv b \pmod{c}$ . Если же  $a + x \equiv a + x'$ , то  $x \equiv x'$  на основании свойства сокращения для сложения. Другим способом выразить то же самое можно, сказав, что классы сравнений по модулю  $c$  образуют *группу* относительно сложения. Нейтральным элементом этой группы является класс всех чисел, делящихся на  $c$ , поскольку если  $k$  делится на  $c$ , то  $a + k \equiv a \pmod{c}$  для всех  $a$ . Так как действие в группе обозначается знаком  $+$ , то естественно для этого нейтрального элемента принять обозначение  $0$  и считать, что сравнение  $k \equiv 0 \pmod{c}$  означает, что  $c$  делит  $k$ . При переходе к умножению обстановка значительно усложняется. Сравнение  $ax \equiv b \pmod{c}$  может иметь решение, а может и не иметь; когда решение есть, оно может оказаться не единственным.

Манипулировать с решением этого сравнения  $ax \equiv b \pmod{c}$  помогает очень важная *китайская теорема об остатках*<sup>1)</sup>. Эта теорема представляет собой следующий шаг за алгоритмом Евклида, и ее можно сформулировать следующим образом. Два натуральных числа называются *взаимно простыми*, если их наибольший общий делитель есть 1. Пусть  $c$  и  $d$  взаимно просты. Если  $a$  и  $b$  — данные натуральные числа, то имеется решение  $x$  задачи:  $x \equiv a \pmod{c}$  и  $x \equiv b \pmod{d}$ . Кроме того, если числа  $x, x'$  оба являются решениями, то  $x \equiv x' \pmod{cd}$ . Это и есть китайская теорема об остатках. Она может быть доказана следующим образом.

Если  $c$  или  $d$  есть 1, то одно из сравнений  $x \equiv a \pmod{c}$ ,  $x \equiv b \pmod{d}$  тривиально и доказываемое утверждение очевидно. Основное предположение о взаимной простоте  $c$  и  $d$  означает, что алгоритм Евклида в конце концов доходит до 1. Будем считать, что  $c_0 = c$ ,  $c_1 = d$ ,  $c_0 = q_1 c_1 + c_2$ ,  $c_1 = q_2 c_2 + c_3$ ,  $\dots$ ,  $c_0 > c_1 > \dots > c_n = 1$ . Так как теорема верна для  $c = c_{n-1}$  и  $d = c_n = 1$ , то достаточно показать, что из случая  $c = c_m$ ,  $d = c_{m+1}$  вытекает случай  $c = c_{m-1}$ ,  $d = c_m$ . Для этого допустим, что  $a, b$  даны. Наша задача состоит в том, чтобы найти натуральное число  $x$ , для которого  $x \equiv a \pmod{c_m}$  и  $x \equiv b \pmod{c_{m-1}}$ . Поскольку  $x + c_m c_{m-1}$  обладает теми же свойствами, что и  $x$ ,

<sup>1)</sup> Я не знаю, откуда произошло это название. Возможно, оно появилось из-за того, что теорема была известна очень давно в Китае. См. Диксон [D2, т. 2, стр. 57].



мы можем предположить, не ограничивая общности, что  $x > b$ . Тогда  $x = b + kc_{m-1}$  для некоторого  $k$ . Значит,  $x = b + k(q_m c_m + c_{m+1}) \equiv b + kc_{m+1} \pmod{c_m}$  и  $x \equiv a \pmod{c_m}$ . Следовательно,  $k$  должно удовлетворять сравнению  $b + kc_{m+1} \equiv a \pmod{c_m}$ . Пусть  $y$  — решение сравнений  $y \equiv b \pmod{c_{m+1}}$  и  $y \equiv a \pmod{c_m}$ . (Такое  $y$  существует по предположению индукции.) Так как  $y + c_m c_{m+1}$  обладает теми же двумя свойствами, что и  $y$ , мы можем предположить, не ограничивая общности, что  $y > b$ . Тогда  $y = b + j$  для некоторого  $j$  и  $j \equiv 0 \pmod{c_{m+1}}$ , т. е.  $y = b + jc_{m+1}$  для некоторого  $j$ . Теперь определим  $x$  условием  $x = b + kc_{m-1}$ . Тогда по модулю  $c_m$  имеем  $x = b + k(q_m c_m + c_{m+1}) \equiv b + kc_{m+1} = y \equiv a$ , а по модулю  $c_{m-1}$  имеем  $x = b + kc_{m-1} \equiv b$ , как и требовалось. Это доказывает, что всегда имеется  $x$  с нужными свойствами. Если  $x$  и  $x'$  оба решают сравнения  $x \equiv a \pmod{c}$ ,  $x \equiv b \pmod{d}$  и если предположить, что  $x > x'$ , то  $x = x' + k$ , где  $k \equiv 0 \pmod{c}$  и  $k \equiv 0 \pmod{d}$ , т. е.  $k$  делится и на  $c$  и на  $d$ , и если  $c$  и  $d$  взаимно просты, то  $k$  делится на  $cd$ . На основании уже доказанной части теоремы имеется такое число  $x$ , что  $x \equiv 0 \pmod{c}$  и  $x \equiv 1 \pmod{d}$ . Иначе говоря,  $x = n_1 c$  и  $x = n_2 d + 1$ . Но  $k$  делится на  $c$ ,  $k = qc$  для некоторого  $q$ . Тогда  $n_1 k = n_1 qc = qx = q(n_2 d + 1) = n_2 qd + q$ . Так как  $d$  делит  $k$ , отсюда следует, что  $d$  делит  $q$ , т. е.  $q = q'd$  и  $k = q'cd$ , что и требовалось доказать.

Очень просто показать, что если  $c$  и  $d$  не взаимно просты, то сравнения  $x \equiv a \pmod{c}$  и  $x \equiv b \pmod{d}$  *никогда* не имеют единственного решения  $x$  по модулю  $cd$ : либо нет ни одного решения, либо решений больше одного. Для этого достаточно заметить, что если наибольший общий делитель чисел  $c$  и  $d$  есть  $D$  и, например,  $c = Dc'$ ,  $d = Dd'$ , то число  $m = Dc'd'$  делится как на  $c$ , так и на  $d$ , но не делится на  $cd$ , поскольку  $cd = D^2 c'd' > m$ . Следовательно, если  $x \equiv a \pmod{c}$ ,  $x \equiv b \pmod{d}$ , то  $x + m$  также удовлетворяет этим сравнениям, но  $x + m \not\equiv x \pmod{cd}$ . Таким образом, если решения есть, то их больше одного, что и требовалось доказать.

Вернемся теперь к решению сравнения  $ax \equiv b \pmod{c}$ . Если  $a$  и  $c$  взаимно просты, то эта задача может быть решена при помощи китайской теоремы об остатках. Именно, решим сравнения  $y \equiv 0 \pmod{a}$ ,  $y \equiv b \pmod{c}$  и положим  $y = ax$ . В частности, сравнение  $az \equiv 1 \pmod{c}$  имеет решение. Следовательно, если  $ax \equiv b$  и  $ax' \equiv b \pmod{c}$ , то  $x \equiv azx \equiv zb \equiv zax' \equiv x' \pmod{c}$  и решение сравнения  $ax \equiv b \pmod{c}$  единственно по модулю  $c$ . С другой стороны, если  $a$  и  $c$  не взаимно просты, то сравнение  $ax \equiv b \pmod{c}$  *никогда* не имеет единственного решения по модулю  $c$  — либо нет ни одного решения, либо решений более одного по модулю  $c$ . Чтобы убедиться в этом, достаточно написать  $a = Da'$ ,  $c = Dc'$ , где  $D > 1$ , и заметить, что  $ac' = a's \equiv 0 \pmod{c}$ , тогда как  $c' \not\equiv 0 \pmod{c}$ , поскольку  $c' < c$ . Тогда из  $ax \equiv b \pmod{c}$

следует, что  $a(x + c') \equiv b \pmod{c}$ , но  $x + c' \not\equiv x \pmod{c}$ . Значит, если решения имеются, то их больше одного.

Натуральное число называется *простым*, если оно взаимно просто со всеми числами, меньшими его самого. (В случае числа 1, когда это условие пусто, добавляется специальное определение, на основании которого число 1 считается *не* простым.) При помощи только что доказанного то же самое можно выразить, сказав, что число  $p$  простое тогда и только тогда, когда  $p > 1$  и сравнение  $ax \equiv b \pmod{p}$  имеет единственное решение  $x$  для всех  $b$  и для всех  $a \not\equiv 0 \pmod{p}$ . Следовательно, в арифметике по простому модулю всегда можно *делить* на ненулевые элементы. В частности, натуральные простые числа обладают следующим основным свойством: если  $p$  делит  $uv$ , то либо  $p$  делит  $u$ , либо  $p$  делит  $v$ . (Если  $uv \equiv 0 \pmod{p}$  и  $u \not\equiv 0 \pmod{p}$ , то путем деления получаем сравнение  $v \equiv 0 \pmod{p}$ .)

*Основная теорема арифметики* устанавливает, что каждое натуральное число, большее <sup>1)</sup> 1, может быть точно одним способом записано в виде произведения простых чисел. Точнее, для данного  $n > 1$  имеется такая конечная последовательность  $p_1, p_2, \dots, p_m$  простых чисел ( $m \geq 1$ ), что  $n = p_1 p_2 \dots p_m$ , и если  $p_1 p_2 \dots p_m = p'_1 p'_2 \dots p'_\mu$ , то  $m = \mu$  и последовательность  $p'_1, p'_2, \dots, p'_\mu$  является лишь перестановкой последовательности  $p_1, p_2, \dots, p_m$ . Эту теорему можно доказать следующим образом.

Будем пытаться делить заданное  $n > 1$  на числа 2, 3, 4,  $\dots$ ,  $n$ . Пусть  $p \leq n$  — первое из чисел, на которое  $n$  разделилось без остатка, скажем  $n = pq$ . Тогда  $n > q$ . Кроме того, число  $p$  должно быть простым, ибо в противном случае либо  $p = 1$ , что уже исключено, либо имеется число  $a < p$ , не взаимно простое с  $p$ . Пусть  $d$  — наибольший общий делитель  $a$  и  $p$ . Тогда  $1 < d$  и  $d \leq a < p$ ; так как  $d$  делит  $p$ , оно делит и  $n = pq$ , а это противоречило бы определению числа  $p$ . Значит,  $p$  простое. Если  $q > 1$ , то те же рассуждения дают  $q = p'q'$ , где  $p'$  — простое и  $q > q'$ . Таким образом,  $n = pp'q'$ . Если  $q' > 1$ , то процесс можно повторить и найти  $n = pp'r''q''$ , где  $q'' < q'$ . На основании принципа бесконечного спуска этот процесс должен завершиться представлением числа  $n$  в виде произведения простых. Если  $p_1 p_2 \dots p_m = p'_1 p'_2 \dots p'_\mu$ , то  $p'_1 p'_2 \dots p'_\mu \equiv 0 \pmod{p_1}$ . Если  $p'_1 \neq p_1$ , то  $p_1$  и  $p'_1$  взаимно просты и сравнение можно разделить на  $p'_1$ , что дает  $p'_2 p'_3 \dots p'_\mu \equiv 0 \pmod{p_1}$ . Таким же образом, если  $p'_2 \neq p_1$ , то  $p'_3 p'_4 \dots p'_\mu \equiv 0 \pmod{p_1}$ . Значит, предположение  $p'_1 \neq p_1, p'_2 \neq p_1, \dots, p'_\mu \neq p_1$  привело бы к сравнению  $1 \equiv 0 \pmod{p_1}$ . Так как  $1 \not\equiv 0 \pmod{p_1}$  (поскольку 1 не является простым числом), то

<sup>1)</sup> Само число 1 пришлось бы рассматривать как произведение *никаких* простых. Для того чтобы была верна эта теорема, число 1 и не считается простым.

отсюда следует, что  $p'_j = p_1$  при некотором  $j$ . Произведя, если необходимо, перестановку последовательности  $p'_1, \dots, p'_\mu$ , мы можем считать, что  $p'_1 = p_1$ . Тогда на основании свойства сокращения получаем  $p_2 p_3 \dots p_m = p'_2 p'_3 \dots p'_\mu$ . Если  $m = 1$ , то это дает  $1 = p'_2 p'_3 \dots p'_\mu$ , откуда  $\mu = 1$  и последовательности  $p_1, p_2, \dots, p_m$  и  $p'_1, p'_2, \dots, p'_\mu$  совпадают. Если  $\mu > 1$ , то такие же рассуждения, как и выше, показывают, что  $p_2$  должно встречаться среди  $p'_2, p'_3, \dots, p'_\mu$ . За счет перестановки можно предположить, что  $p'_2 = p_2$ , и заключить, что  $p_3 p_4 \dots p_m = p'_3 p'_4 \dots p'_\mu$ . Если  $m = 2$ , то  $\mu = 2$  и последовательности совпадают. В противном случае после перестановки мы получаем  $p_4 p_5 \dots p_m = p'_4 p'_5 \dots p'_\mu$ , и т. д. По принципу бесконечного спуска мы в конце концов придем к заключению, что посредством перестановки последовательности  $p'_1, p'_2, \dots, p'_\mu$  можно добиться того, что эти две последовательности совпадут.

Натуральные числа являются, конечно, теми объектами, которым в первую очередь подходит название «число», и недаром древние греки применяли название «число» только к натуральным числам. Даже во времена Ферма дроби, иррациональные величины, нуль и отрицательные величины не пользовались всеобщим признанием как «числа». Однако во многих ситуациях удобнее иметь более широкое понятие числа. Например, после нескольких первых параграфов этой книги стало удобнее иметь дело с *целыми*, а не только с натуральными числами. Целые числа — это натуральные  $1, 2, 3, \dots$  вместе с отрицательными  $-1, -2, -3, \dots$  и нулем  $0$ . В терминах целых чисел удалось придать Последней теореме Ферма более симметричный вид: «если  $p$  — нечетное простое число, то равенство  $x^p + y^p + z^p = 0$  невозможно в целых числах  $x, y, z$ , за исключением тривиального случая, когда одно из трех неизвестных равно нулю». Такая формулировка облегчила бы Эйлеру доказательство случая  $p = 3$ , поскольку отпала бы необходимость отдельно рассматривать случаи четного и нечетного  $z$  в равенстве  $x^3 + y^3 = z^3$ .

Основные свойства целых чисел являются простыми обобщениями соответствующих свойств натуральных чисел и, поскольку в наши дни целые числа вводятся в начальной школе, едва ли необходимо обсуждать их здесь более подробно.

## Упражнения

1. Докажите, что если  $d$  делит как  $a$ , так и  $b$ , то оно делит и  $a + b$ . Более того, оно делит  $qa + rb$  для любых  $q$  и  $r$ .
2. Докажите, что если  $a$  делит  $b$  и  $b$  делит  $a$ , то  $a = b$ .
3. Докажите при помощи алгоритма Евклида, что если  $d$  — наибольший общий делитель чисел  $a$  и  $b$ , то либо существуют такие натуральные числа  $u$  и  $v$ , что  $ua = d + vb$ , либо существуют такие натуральные числа  $u$  и  $v$ , что  $d + ua = vb$ . [Обработайте алгоритм с конца, как это делалось

в тексте при доказательстве китайской теоремы об остатках.] Выведите отсюда, что если  $a$  и  $b$  взаимно просты, то либо сравнение  $ax \equiv 1 \pmod{b}$ , либо сравнение  $ax + 1 \equiv 0 \pmod{b}$  имеет решение  $x$ . Покажите, что во втором случае сравнение  $ax \equiv 1 \pmod{b}$  имеет некоторое решение  $x$ . Следовательно, если  $a$  и  $b$  взаимно просты, то сравнения  $y \equiv 0 \pmod{a}$ ,  $y \equiv 1 \pmod{b}$  всегда имеют решение. Выведите отсюда китайскую теорему об остатках.

4. Найдите все решения следующих пар сравнений:

$$(a) \quad x \equiv 3 \pmod{46}, \quad x \equiv 4 \pmod{52};$$

$$(b) \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7};$$

$$(c) \quad x \equiv 7 \pmod{56}, \quad x \equiv 2 \pmod{295}.$$

5. Покажите, что существуют такие натуральные числа  $y$  и  $z$ , что решение задачи в китайской теореме об остатках дается формулой  $x = ay + bz$ . Таким образом, числа  $y$  и  $z$  представляют собой арифметический эквивалент «разбиения единицы», показывающий, что может быть найдено целое число  $x$ , принимающее произвольно заданные «значения по отношению к  $c$  и  $d$ ».

6. Докажите, что если  $c_1, c_2, \dots, c_n$  попарно взаимно просты и  $a_1, a_2, \dots, a_n$  — произвольные целые числа, то имеется такое целое число  $x$ , что  $x \equiv a_i \pmod{c_i}$  для  $i = 1, 2, \dots, n$ .

7. Пусть  $a, b$  и  $c$  — заданные целые числа. Используя алгоритм Евклида, опишите процедуру нахождения всех (целых) решений  $x$  и  $y$  уравнения  $ax + by + c = 0$ . [Если  $a$  или  $b$  есть нуль, то задача тривиальна. Можно предположить, не умаляя общности, что  $a$  и  $b$  положительны. Если  $d$  — их наибольший общий делитель, то задача тогда и только тогда имеет решение, когда  $d$  делит  $c$ . При  $c = 0$  и взаимно простых  $a$  и  $b$  это легкая задача.]

## А.2. Примитивные корни по модулю $p$

Натуральное число  $g$  называется *примитивным корнем* по модулю простого числа  $p$ , если степени  $g, g^2, g^3, \dots$  исчерпывают все возможности по модулю  $p$  для целых чисел, взаимно простых с  $p$ . То есть  $g$  является примитивным корнем по модулю  $p$ , если для любого натурального числа  $k$  либо  $k \equiv 0 \pmod{p}$ , либо существует такое натуральное число  $j$ , что  $k \equiv g^j \pmod{p}$ . В гл. 4, 5 и 6 мы постоянно пользовались тем, что для любого простого числа  $p$  существует хотя бы один примитивный корень по модулю  $p$ . Следующее доказательство этого утверждения является одним из двух его доказательств, приведенных Гауссом в *Disquisitiones Arithmeticae*. Гаусс утверждает (разд. 56), что его предшественники строго не сформулировали и не доказали эту теорему, хотя они и знали (или думали, что знали), что эта теорема верна.

В § 1.8 было показано, что для каждого целого  $a \not\equiv 0 \pmod{p}$  существует такое натуральное число  $d$ , что  $a^d \equiv 1 \pmod{p}$ , и из сравнения  $a^j \equiv 1 \pmod{p}$  следует, что  $d \mid j$ . Это натуральное число  $d$  называется *порядком*  $a$  по модулю  $p$ . Согласно теореме Ферма, порядок  $a$  по модулю  $p$  делит  $p - 1$ . Надо доказать, что существует хотя бы одно  $a$ , порядок которого по модулю  $p$  равен  $p - 1$ . Гаусс доказывает это путем построения такого целого числа.

Пусть  $p-1 = p_1 p_2 \dots p_m$  — разложение  $p-1$  на простые множители. Пусть  $q$  — одно из простых чисел  $p_1, p_2, \dots, p_m$ ; пусть  $v$  — кратность, с которой это число входит в разложение. Рассуждение с последовательными разностями из § 2.4 показывает, что сравнение  $x^{(p-1)/q} - 1 \equiv 0 \pmod{p}$  не может выполняться для всех целых чисел  $x = 1, 2, 3, \dots, p-1$ . (Если бы все эти числа удовлетворяли сравнению, то, взяв разности, мы получили бы, что  $p$  делит  $((p-1)/q)!$ . Но это невозможно, поскольку  $p$  — простое число, большее всех делителей  $((p-1)/q)!$ .) Следовательно, существует такое целое число  $b$ ,  $0 < b < p$ , что  $b^{(p-1)/q} \not\equiv 1 \pmod{p}$ . Пусть  $c$  — целое по модулю  $p$ , полученное возведением  $b$  в  $((p-1)/q^v)$ -ю степень. Утверждение состоит в том, что порядок  $c$  равен  $q^v$ . Так как, согласно теореме Ферма,  $c^{q^v}$  равно  $b^{p-1} \equiv 1 \pmod{p}$ , то порядок  $c$  должен делить  $q^v$ . Отсюда следует, что порядок  $c$  не делится ни на одно простое, отличное от  $q$ , т. е. порядок  $c$  равен степени  $q$ . Для доказательства того, что этот порядок равен  $q^v$ , достаточно доказать, что  $c^{q^{v-1}} \not\equiv 1 \pmod{p}$ , но это немедленно следует из способа выбора  $c$  и  $b$ .

Допустим, что такое целое число  $c$  найдено для каждого простого делителя  $q$  числа  $p-1$ , скажем  $c_1, c_2, \dots, c_n$ ; пусть  $g$  — произведение этих чисел. (Здесь  $n \leq m$  — число различных простых делителей числа  $p-1$ .) Утверждение состоит в том, что порядок  $g$  равен  $p-1$ . Если бы порядок  $g$  был отличен от  $p-1$ , то он был бы собственным делителем  $p-1$ . Таким образом, нашелся бы простой делитель  $q$  числа  $p-1$ , который делит порядок  $g$  с меньшей кратностью, чем он делит  $p-1$ . Тогда порядок  $g$  делил бы  $(p-1)/q$ , и отсюда следовало бы, что  $g^\mu \equiv 1 \pmod{p}$ , где  $\mu = (p-1)/q$ . Не ограничивая общности, можно считать, что  $c$ , соответствующее этому  $q$ , равно  $c_1$ . Тогда  $c_2^\mu \equiv c_3^\mu \equiv \dots \equiv c_n^\mu \equiv 1 \pmod{p}$ , поскольку порядки этих целых чисел делят  $\mu = (p-1)/q$ . Отсюда следовало бы, что  $1 \equiv g^\mu \equiv c_1^\mu$ , что является противоречием, так как  $q^v$  не делит  $\mu$ . Таким образом, порядок  $g$  равен  $p-1$ , что и требовалось показать.

## Упражнения

1. Подбором найдите примитивные корни для нескольких простых. Обширные таблицы примитивных корней можно найти в знаменитом труде Якоби *Canon Arithmeticus* [J3], а также во многих других книгах.

2. Пусть  $\gamma$  — примитивный корень по модулю  $p$ . Покажите, что  $\gamma^k$  является примитивным корнем по модулю  $p$  тогда и только тогда, когда  $k$  взаимно просто с  $p-1$ . Найдите все примитивные корни для всех простых, меньших 20.

3. Прочитайте и перескажите своими словами другое доказательство Гаусса существования примитивных корней [*Disquisitiones Arithmeticae*, Art. 54].



## ОТВЕТЫ К УПРАЖНЕНИЯМ

- 1.3. 1. Равенство  $2p^2 = 4961 + 8161$  дает  $p = 81$ ; тогда  $q = 40$ .
- 1.6. 1. См. упр. 3 к § 1.3. 2. Если бы выполнялось равенство  $x^4 - y^4 = z^2$ , то пифагоров треугольник  $(x^4 - y^4, 2x^2y^2, x^4 + y^4)$  имел бы площадь, равную квадрату.
- 1.7. 1.  $x, y$  имеют противоположную четность. Если  $x$  четно, то  $x^2$  имеет вид  $4k$ , если  $x$  нечетно, то  $x^2 = 4k + 1$ . 2. Если  $p = x^2 + 3y^2$ , то  $x = 3k + 1$  и  $x^2 = 3n + 1$ . Если  $3m + 1$  — простое, то  $m$  — четное. 3.  $(2n + 1)^2$  имеет вид  $8k + 1$ ;  $2y^2 = 8k$  или  $8k + 2$ . 4. Число  $n$  удовлетворяет условиям Жирара тогда и только тогда, когда любое простое число  $p$  вида  $4m + 3$ , делящее  $n$ , входит в разложение  $n$  с четной кратностью.
- 1.8. 1.  $p = 74k + 1$ . Если  $p = 149$ , то остатки чисел  $2^5, 2^8, 2^{16}, 2^{32}, 2^{37}$  равны 32, 107,  $-24, -20$  и  $-44 \not\equiv 1$  соответственно. Если  $p = 223$ , то остаток числа  $2^{37}$  равен 1. 2.  $a^{2n+1} + b^{2n+1} = (a + b)(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - \dots + b^{2n})$ . Если  $p \nmid x$ , то  $x^{p-1} = kp + 1$ . 3.  $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30$ .
- 1.9. 3.  $pQ - Pq = (p^2 + pqr - pqr - q^2A)/|k| = \text{sgn}(k)$ ;  $Q(QA + PR) = P^2 - K + PQR$  делится на  $K$ . Поэтому  $QA + PR$  делится на  $K$ . 4.  $P - rQ = -qs/|k| = \pm qK$ . Так как  $P + RQ = nK$ , то  $K \mid (r + R)Q$  и  $K \mid (r + R)$ . 5. В циклическом методе второе  $r = 13$  определяется условиями  $5 \mid (12 + r)$  и  $r^2 - 149$  — малое число. Следующее  $k$  равно  $(13^2 - 149)/(-5) = -4$ . Последовательность  $k$  имеет вид 1,  $-5, -4, 7, -7, 4, 5, -1, 5, 4, -7, 7, -4, -5, 1$ . В английском методе второе  $r$  равно 8 и последовательность  $k$  имеет вид 1,  $-5, 17, -4, 7, -7, 4, \dots, 17, -5, 1$ . 6.  $|K| \mathcal{P} = PR + QA = P(R + r) - rP + QA = Pn \mid K| - rP + QA$ . Таким образом,  $\mathcal{P} = nP + x$ , где  $|k| \mid K| x = -r(pr + qA) + A(p + qr) = p(A - r^2) = -ps$ . Так как  $|k| \mid K| = |s|$ , то  $x = -\text{sgn}(s) \cdot p$ . Вычисление  $\mathcal{Q}$  аналогично. 7.  $P - rQ$  делится как на  $k$ , так и на  $K$  (упр. 4). Таким образом,  $pQ + qP$  делится на  $k$  и  $K$  тогда и только тогда, когда  $pQ + qrQ$  делится на  $k$  и  $K$ . Как  $p + qr$ , так и  $pr + Aq$  делятся на  $k$  (упр. 3). 9.  $K$  и  $k$  имеют противоположные знаки и  $kK = r^2 - A$ . Если  $k < 0$ , то знак  $(-r + K)^2 - A = K(k - 2r + K)$  совпадает со знаком  $k - 2r + K = [(r + |k|)^2 - A]/k < 0$ ;  $(-r + 2K)^2 - A = K(k - 4r + 4K)$  положительно, поскольку  $k - 2r + 2K = k^{-1}[(r + |k|)^2 - A - (A - r^2)]$ . Случай  $k > 0$  рассматривается аналогично и  $(R^2 - A)/K = [(r + |k|)^2 - A]/k$ , поскольку обе части равны  $k + 2r \text{sgn}(k) + K$ . 10. Следующее  $r$  — обозначим его  $R$  — определяется условиями:  $R = -r + nK, R^2 < A, R$  как можно больше. Если  $K < 0$ , то  $kK + 2rK + K^2 < 0, r^2 - A + 2rK + K^2 < 0, (-r + |K|)^2 < A$ . Это неравенство справедливо и при  $K > 0$ . Таким образом,  $R \geq -r + |K|, -r \leq R - |K| \leq R$  и  $(R - |K|)^2 < A$ . С другой стороны,  $(R + |K|)^2 > A$ . При  $\mathcal{K} = (R^2 - A)/K$  отсюда следует, что  $R^2 -$



—  $2R \mid K \mid + K^2 < A$ ,  $K (\mathcal{K} - 2R \operatorname{sgn}(K) + K) < 0$ . Это дает  $\mathcal{K} + 2R + K > 0$  при  $K < 0$  и  $\mathcal{K} - 2R + K < 0$  при  $K > 0$ . Противоположные неравенства получаются аналогичным образом из  $(R + \mid K \mid)^2 > A$ . 11.  $r$  имеет вид  $-R + nK$ . Это вместе с неравенствами  $r^2 < A$ ,  $(r + \mid K \mid)^2 > A$  определяет  $r$ , когда известны  $R$  и  $K$ . Неравенства  $-A < kK < 0$  показывают, что для  $k$  имеется только конечное число возможностей. Первое  $k$  равно 1, поэтому при первом повторении получается 1. 13. Легко доказать равенство  $x_{i+1}y_i - y_{i+1}x_i = \pm 1$  — сначала для положительных, а затем и для всех  $i$ . Равенство  $x_{i+1}x_i - Ay_{i+1}y_i = \operatorname{sgn}(k_i) r_i$  (где  $r_i$  — значение  $r$ , которое используется при переходе от  $x_i, y_i$  к  $x_{i+1}, y_{i+1}$ ) легко доказывается при положительных  $i$ . Затем оно получается при всех  $i$  ( $n_{i+1} \mid k_{i+1} \mid = r_i + r_{i+1}$ ). Тогда  $(x_i^2 - Ay_i^2) \cdot (x_{i+1}^2 - Ay_{i+1}^2) = (x_i x_{i+1} - Ay_i y_{i+1})^2 - A(x_{i+1}y_i - y_{i+1}x_i)^2 = r_i^2 - A = k_i k_{i+1}$ , поэтому равенство  $x_i^2 - Ay_i^2 = k_i$  выполняется при всех  $i$ .

1.10. 1. Уравнение имеет вид  $(1 + x)(1 + x^2) = y^2$ . Тогда  $x \geq -1$ . Так как  $1 + x^2$  не является квадратом при  $x \neq 0$ , то  $1 + x$  и  $1 + x^2$  не взаимно просты. В действительности  $1 + x = 2u^2$ ,  $1 + x^2 = 2v^2$  при  $x > 0$ . Тогда  $(u^2, u^2 - 1, v)$  — примитивная пифагорова тройка, если  $(u, x) \neq (1, 1)$ . Если  $x > 1$  и  $u$  нечетно, то  $u^2 = p^2 - q^2$ ,  $u^2 - 1 = 2pq$ ,  $v = p^2 + q^2$ , где  $p$  и  $q$  — взаимно простые числа разной четности и  $p > q$ . Тогда  $1 = (p - q)^2 - 2q^2$  и  $p - q$  является квадратом. Таким образом,  $(q^2 + 1)^2 = q^4 + t^4$ , что невозможно. Если  $u$  четно, то  $u^2 = 2pq$ ,  $u^2 - 1 = p^2 - q^2$  и  $v = p^2 + q^2$ . Тогда  $p$  четно и в действительности  $p = 2t^2$ . Значит,  $1 = (p + q)^2 - 2p^2$ ,  $8t^4 = (p + q - 1)(p + q + 1)$ ,  $2t^4 = a(a + 1)$ . Одно из чисел  $a, a + 1$  является 4-й степенью, а другое представляет собой удвоенную 4-ю степень. Отсюда следует, что  $b^4 - 2c^4 = \pm 1$ . При знаке «+» в этой формуле для  $d = c^2$  выполняется равенство  $(d^2 + 1)^2 = d^4 + b^4$ , что невозможно. Следовательно,  $(d^2 - 1)^2 = d^4 - b^4$ . Ясно, что  $b \neq 0$ . Таким образом,  $b^4 = d^4$ . Но  $b$  и  $c$  взаимно просты, поэтому  $b = \pm 1$ ,  $c = \pm 1$ ,  $a = b^4 = 1$ ,  $a + 1 = 2c^4 = 2$ ,  $p + q = 3$ ,  $p = 2$ ,  $u^2 = 4$ ,  $x = 7$ .

2.3. 1. Каждая единица имеет вид  $\pm (1 + \sqrt{2})^n$  при некотором целом  $n$ ;  $((1 + \sqrt{2})^{-1} = -(1 - \sqrt{2}))$ . Единственными единицами вида  $x + y\sqrt{-41}$  или  $x + y\sqrt{-7}$  являются  $\pm 1$ . Равенство  $8^2 = 1 + 7 \cdot 3^2$  дает единицы  $\pm (8 + 3\sqrt{-7})^n$ , где  $(8 + 3\sqrt{-7})^{-1} = 8 - 3\sqrt{-7}$ . В этом случае так получаются все единицы, поскольку равенство  $x^2 = -1 + 7y^2$  невозможно по модулю 8. Единственными единицами вида  $x + y\sqrt{-1}$  являются  $\pm 1$  и  $\pm \sqrt{-1}$ . 2.  $4\sqrt{2} + \sqrt{5} = (19 + 6\sqrt{10})(2\sqrt{2} - \sqrt{5})^3$ .

2.4. 1. Пусть  $P = p^2 + q^2 = a^2 + b^2$ . При необходимости измените знак  $q$  таким образом, чтобы  $P$  делило  $pb + aq$ . Тогда либо  $ap - bq = 0$  и  $aq + bp = \pm P$ , либо  $ap - bq = \pm P$  и  $aq + bp = 0$ . Таким образом, или  $a = \pm q$ , или  $a = \pm p$ . Аналогичные рассуждения проходят и в остальных случаях. 2. Согласно формуле бинома Ньютона,  $(x + 1)^n - x^n = nx^{n-1} +$  члены низшей степени. (Также и  $x^n - (x - 1)^n = nx^n + \dots$ ) Таким образом, первые разности  $ax^n + bx^{n-1} + \dots + c$  равны  $anx^{n-1} + \dots$ . 8. Указанное деление возможно тогда и только тогда, когда  $P$  делит  $(ap \mp bq) \pm (aq \pm bp) i$ . 10. Согласно упр. 1,  $p = u^2 + v^2$ . Если  $r$  является обратным к  $v$  по модулю  $p$ , то сравнение  $a^2 \equiv -1 \pmod{p}$  имеет решение  $a = ru$ . Аналогично, согласно упр. 7, сравнение  $b^2 \equiv -2 \pmod{p}$  разрешимо.

Тогда по теореме Ферма  $2^{(p-1)/2} \equiv (a^2 b^2)^{(p-1)/2} \equiv 1 \pmod{p}$ . Так как 64 является наименьшей степенью 2, сравнимой с 1 по модулю  $p$ , то  $(p-1)/2 = 64k$ ,  $p = 1 + 128k$ . 11.  $2^{32} - 1 = (2^{16} + 1)(2^8 + 1) \times \times (2^4 + 1)(2^2 + 1)(2 + 1)(2 - 1)$ . Следовательно,  $257 = 2^8 + 1$  не делит  $2^{32} - 1 + 2$ .

2.5. 1. Из равенства  $x + \sqrt{-2} = (a + b\sqrt{-2})^3$  следует, что  $b(3a^2 - 2b^2) = 1$ ,  $b = \pm 1$ ,  $a = \pm 1$ . Тогда  $x = \pm 7$  или  $\pm 5$ . 4.  $(1 \pm \sqrt{-3})^2$  делится на 2. 5.(а) Равенство  $(2 + \sqrt{-3})(1 \pm 2\sqrt{-3})$  дает два единственно возможных представления  $4^2 + 3 \cdot 5^2$ ,  $8^2 + 3 \cdot 3^2$ . (b)  $(2 + \sqrt{-3}) \times \times (2 \pm \sqrt{-3})$  дает  $49 = 7^2 = 1^2 + 3 \cdot 4^2$ . (с) Найдите представления  $112 = 336/3$ . Они получаются из  $4(2 + \sqrt{-3})$  и  $2(2 + \sqrt{-3}) \times \times (1 + \sqrt{-3})$ . Искомые представления имеют вид  $336 = 3 \cdot 8^2 + + 3^2 \cdot 4^2 = 3 \cdot 2^2 + 3^2 \cdot 6^2 = 3 \cdot 10^2 + 3^2 \cdot 2^2$ .

3.2. 2. Воспользуйтесь тем фактом, что целое число  $\not\equiv 0 \pmod{p}$  обратимо по модулю  $p$ . 3. 13-ми степенями по модулю  $4 \cdot 13 + 1$  являются 0,  $\pm 1$ ,  $\pm 30$ ; 17-ми степенями по модулю  $6 \cdot 17 + 1$  являются 0,  $\pm 1$ ,  $\pm 46$ ,  $\pm 47$ , и условия теоремы Софи Жермен не выполняются. Однако 17-ми степенями по модулю  $8 \cdot 17 + 1$  являются 0,  $\pm 41$ ,  $\pm 37$ ,  $\pm 10$ ,  $\pm 1$ . Для 19 первым простым числом, подлежащим испытанию, оказывается 191, по модулю которого 19-ми степенями являются 0,  $\pm 7$ ,  $\pm 49$ ,  $\pm 39$ ,  $\pm 1$ . 4.  $(j + 5)^5 \equiv j^5 \pmod{25}$ . Таким образом, ненулевыми 5-ми степенями по модулю 25 являются 1,  $2^5 \equiv 7$ ,  $3^5 \equiv (-2)^5 \equiv \equiv -7$ ,  $4^5 \equiv -1$ .

4.2. 3. Возьмите  $a_2 = 0$ . Тогда  $A = 2a_0 - a_1$ ,  $B = a_1$ . 4.  $A = b + c$ ,  $B = b - c$ . Степени единицы  $\theta_0$  различны, поскольку  $\theta_0^n = \pm a_n \mp \mp a_{n+1}\theta_0 \neq 1$ , где  $a_{n+1} = a_n + a_{n-1}$ . 6.  $f(\alpha) = g(\alpha)$  означает, что  $f(\alpha)$  идентично  $g(\alpha) + c(1 + \alpha + \dots + \alpha^{\lambda-1})$ . Таким образом,  $f(1) = g(1) + c\lambda$ ;  $Nf(\alpha) \equiv f(1)f(1^2) \dots f(1^{\lambda-1}) = f(1)^{\lambda-1} \equiv 0$  или  $1 \pmod{\lambda}$ . 8. Композиция сопряжений  $\alpha \mapsto \alpha^j$  и  $\alpha \mapsto \alpha^k$  дает  $\alpha \mapsto \alpha^n$ , где  $n = jk$ . Если ни  $j$ , ни  $k$  не являются нулем по модулю  $\lambda$ , то  $n \not\equiv \equiv 0 \pmod{\lambda}$ . Обратным к сопряжению  $\alpha \mapsto \alpha^j$  является  $\alpha \mapsto \alpha^m$ , где  $mj \equiv 1 \pmod{\lambda}$ . 9. Если  $k \equiv -1 \pmod{p}$ , то  $\lambda \equiv 0 \pmod{p}$ ,  $\lambda = p$ . Если  $k^\lambda \equiv -1$  и  $k \not\equiv -1$ , то  $(-k)^\lambda \equiv 1$ ,  $\lambda \mid (p-1)$  по теореме Ферма. 14. Из  $Nf(\alpha) \cdot Ng(\alpha) = 1$  вытекает  $Nf(\alpha) = \pm 1$ . Таким образом,  $Nf(\alpha) = 1 = g(\alpha)f(\alpha)$ . Сократите на  $f(\alpha)$ . 15.  $r(\alpha) = 0$ , поскольку  $h(\alpha) = f(\alpha) = 0$ . Если  $f(X)$  делится на  $p$ , то  $f/p$  обладает теми же свойствами, что и  $f$ ;  $(j-1)h(j) = j^\lambda - 1$ . См. упр. 1 к § 3.2. 16. Если  $f(\alpha)g(\alpha) = 0$  и  $ah(X) = q(X)f(X) + r(X)$ , то  $r(\alpha)g(\alpha) = 0$  и  $r(\alpha)$  может заменить  $f(\alpha)$ , если  $r(X) \neq 0$ . 18. Если  $p(\alpha)$  простое и  $p(\alpha) = f(\alpha)g(\alpha)$ , то  $p(\alpha)$  делит  $f(\alpha)$  или  $g(\alpha)$  и второй сомножитель является единицей.

4.3. 3. Из того что  $h(\alpha)$  неразложимо, но не просто, вытекает, что  $q(\alpha)h(\alpha) = = f(\alpha)g(\alpha)$ , где  $f(\alpha)$ ,  $g(\alpha)$  не делятся на  $h(\alpha)$ . Запишите  $q(\alpha)$ ,  $f(\alpha)$ ,  $g(\alpha)$  в виде произведения неразложимых и заметьте, что  $h(\alpha)$  справа не встречается. Хотя, казалось бы, очевидно, что каждое круговое целое является произведением неразложимых — ведь можно разлагать до тех пор, пока дальнейшее разложение станет невозможным, — доказать это конструктивным способом непросто. 5.  $x^\lambda + y^\lambda \equiv \equiv 0 \pmod{p}$ . Если  $y \not\equiv 0 \pmod{p}$ , то это дает  $(-x/y)^\lambda \equiv 1 \pmod{p}$  и  $\lambda \mid (p-1)$ . С другой стороны,  $x \not\equiv 0 \pmod{p}$ . 6. (а) 1, 11, 31, 61,  $11^2$ ,  $5 \cdot 11$ , 211,  $5 \cdot 41$ ,  $11 \cdot 41$ ,  $11 \cdot 191$ ,  $11 \cdot 191$ . (b) 43, 127, 547, 1093, 463,

29.71, 29.113, 43.127, 7.379, 14.197, 29.449, 7.1597, 10.039, 10.501.  
 8.  $p \mid N(\alpha - k)$  для некоторого  $k$ . Таким образом,  $h(\alpha)$  делит бином и результат следует из теоремы в тексте. 10. (а)  $\alpha \equiv k \pmod{h(\alpha)}$ . Таким образом,  $k^\lambda \equiv \alpha^\lambda = 1 \pmod{h(\alpha)}$ ,  $k^\lambda \equiv 1 \pmod{p}$ ;  $k \not\equiv 1 \pmod{p}$ , поскольку из  $\alpha \equiv 1 \pmod{h(\alpha)}$  вытекало бы  $p \mid N(\alpha - 1) = \lambda$ . По той же причине  $k^2, k^3, \dots, k^{\lambda-1} \not\equiv 1 \pmod{p}$ . Таким образом,  $k^i \equiv k^{i+j}$  для  $0 < j < \lambda$ . Если  $m^\lambda \equiv 1$  и  $m \not\equiv 1 \pmod{p}$ , то  $p \mid N(m - \alpha)$ ,  $h(\alpha)$  делит один из сомножителей  $m - \alpha^j$  нормы  $N(m - \alpha)$ ,  $m \equiv \alpha^j \equiv k^j \pmod{h(\alpha)}$ ,  $m \equiv k^j \pmod{p}$ . (b) Пусть  $p - 1 = \lambda\mu$ . Тогда сравнение  $k^\lambda \equiv 1 \pmod{p}$  имеет не больше  $\lambda$  решений на основании упр. 1 из § 3.2. Также и  $k^\mu \equiv 1 \pmod{p}$  имеет не больше  $\mu$  решений. Пусть  $a^\mu \not\equiv 1 \pmod{p}$ , и положим  $b = a^\mu$ . Тогда все степени элемента  $b$  являются решениями. Если  $d$  — наименьшее целое, для которого  $b^d \equiv 1 \pmod{p}$ , то  $d \mid \lambda$ ,  $d \neq 1$ ,  $d = \lambda$ . 11. По модулю тех простых  $p$ , для которых  $1 + 7 + 7^2 + 7^3 + 7^4 = (7^5 - 1)/(7 - 1) = 2801 \equiv 0 \pmod{p}$ , т. е. только для  $p = 2801$ . 12. В любом случае  $f(X) - g(X) = q(X)(X^{\lambda-1} + \dots + 1) + r(X)$ , где  $\deg r < \lambda - 1$ . Тогда из  $r(\alpha) = 0$  следует  $r(X) = 0$ .

4.4. 8. Хороший способ контролировать вычисления значений  $f(k), f(k^2), f(k^4), \dots, f(k^7)$  по модулю 599 дает тот факт, что их сумма равна 10 по модулю 599. 10. Так как  $(\alpha - 1) \mid \lambda \mid Ng(\alpha)$ ,  $\alpha - 1$  простое, то  $\alpha - 1$  делит некоторое сопряженное элемента  $g(\alpha)$ . Тогда некоторое сопряженное элемента  $\alpha - 1$  делит  $g(\alpha)$ ;  $\alpha - 1$  делит все свои сопряженные. 11. Умножение каждой части равенства на  $\alpha - 1$  дает  $\lambda$ , поэтому обе части равны. Иначе об этом см. в § 6.17.

4.5. 1. См. табл. 4.7.1. 2.  $\theta_0 = \alpha + \alpha^2 + \alpha^4$ ;  $\theta_0\theta_1 = 2$ ;  $f(\alpha)f(\alpha^2)f(\alpha^4) = a + b\theta_0$  для некоторых целых  $a, b$ ;  $Nf(\alpha) = (a + b\theta_0)(a + b\theta_1) = a^2 - ab + 2b^2 = 1/4[(2a - b)^2 + 7b^2]$ . 3.  $(\theta_0 - \theta_1)^2 = \lambda$ , если  $\lambda \equiv 1 \pmod{4}$ , и  $-\lambda$ , если  $\lambda \equiv 3 \pmod{4}$ . 4.  $(\theta_0 + \theta_1)^2 - (\theta_0 - \theta_1)^2 = 4\theta_0\theta_1$ . Значит, достаточно найти  $\theta_0\theta_1$ . Прямым вычислением получаем  $\theta_0\theta_1 = a + b\theta_0 + b\theta_1$ , где  $a$  равно 0 или  $(\lambda - 1)/2$ . Это определяется четностью  $a$ . См. § 5.6. 6. Определите периоды, используя  $\gamma = 3$ . Тогда  $\eta_0^2 = 4 + 2\eta_1 + \eta_2$ ,  $\eta_0\eta_1 = 2\eta_0 + \eta_2 + \eta_3$ ,  $\eta_0\eta_2 = \eta_0 + \eta_1 + \eta_2 + \eta_3 = -1$ ,  $\eta_0\eta_3 = \eta_1 + \eta_2 + 2\eta_3$ . 7. Тогда и только тогда, когда  $p$  имеет вид  $p \equiv g^k$ , где  $g$  — примитивный корень по модулю  $\lambda$ ,  $e \mid k$ . Иными словами,  $p^f \equiv 1 \pmod{\lambda}$ . 8.  $\eta_0$  — период, содержащий  $\alpha$ .

4.6. 2.  $X(X - 1) \dots (X - 10) = X^{11} - 55X^{10} + 1320X^9 - 18150X^8 + 157773X^7 - 902055X^6 + 3416930X^5 - 8409500X^4 + 12753576X^3 - 10628640X^2 + 3628800X$ . Следствие: если  $p$  — простое, то  $(p - 1)! \equiv -1 \pmod{p}$ . Это теорема Вильсона. 3. Если  $\lambda = 13$  и  $p = 3$ , то  $\eta_0^3 = 6 + \eta_0 + 3\eta_1 + 3\eta_3$ . 4. Если  $k \equiv 1 \pmod{p}$ , то  $\lambda \equiv 0 \pmod{p}$ . В противном случае  $k^\lambda \equiv 1 \pmod{p}$  и  $\lambda \mid (p - 1)$ . 5. Если  $\lambda = 5$ , то  $\theta_0^2 = 2 + \theta_1$ ,  $\theta_0^2 + \theta_0 = 1$ ;  $u = 4$  удовлетворяет сравнению  $u^2 + u \equiv 1 \pmod{19}$ ;  $(\theta_0 - 4)(\theta_1 - 4) = 19$ . 6. См. § 4.7;  $\eta_0\eta_1\eta_2\eta_3 = 3$ , когда  $\lambda = 13$ . 7. Если  $f(\alpha) \mid g(\alpha)$ , то  $Nf(\alpha) \mid p^f$  и  $Nf(\alpha)$  — степень числа  $p$ . Так как  $Nf(\alpha) \equiv 0$  или 1 по модулю  $\lambda$ , то  $Nf(\alpha) = 1$  или  $p^f$ .

4.7. 1.  $(\eta_0 + 3)/(\eta_2 - \eta_1 + 1) = -\eta_1$ ;  $1/(-\eta_1) = 1 + \eta_2$ . 3. Одно разложение имеет вид  $(3 - \eta_0 - 2\eta_2)(3 - \eta_2 - 2\eta_0) = 17 - 12\theta_0$ ,  $(17 - 12\theta_0)(17 - 12\theta_1) = 61$ . 4.  $109 = (10 - \theta_0)(10 - \theta_1)$ . 5.  $53 = N(1 + \alpha + \alpha^3)$ . Разложение числа 103 требует решения  $u = 12$  сравнения  $u^6 + u^5 - 5u^4 - 4u^3 + 6u^2 + 3u - 1 \equiv 0 \pmod{103}$ . Тогда

сравнительно легко обнаружить, что произведение шести различных сопряженных элемента  $2(\alpha + \alpha^{12}) + (\alpha^6 + \alpha^7) - 1$  равно 103. Число 3 было разложено в тексте; 5 есть произведение трех сопряженных элемента  $-1 - (\alpha + \alpha^8 + \alpha^{12} + \alpha^5)$ ;  $17 = (4 - \theta_0)(4 - \theta_1)$ ; 7 неразложимо.

- 4.8. 1. В обоих случаях (a) и (b) имеем  $\alpha^2 - \eta_0\alpha + 1 = 0$ , где  $\eta_0 = \alpha + \alpha^4$  для (a) и  $\eta_0 = \alpha + \alpha^6$  для (b). (c)  $\alpha^5 - \theta_0\alpha^4 - \alpha^3 + \alpha^2 + \theta_1\alpha - 1 = 0$ . (d)  $\alpha^3 - \eta_0\alpha^2 + \eta_2\alpha - 1 = 0$ . (e)  $\alpha^5 - \eta_0\alpha^4 + (\eta_1 + \eta_2)\alpha^3 - (\eta_4 + \eta_5)\alpha^2 + \eta_3\alpha - 1 = 0$ . 2. Произведение первых двух равно  $\alpha^6 - 11\alpha^5 - 25\alpha^4 - 155\alpha^3 + 71\alpha^2 - 17\alpha + 1 \equiv \alpha^6 - 11\alpha^5 + 4\alpha^4 - 10\alpha^3 + 13\alpha^2 + 12\alpha + 1$ , а произведение вторых двух имеет такие же коэффициенты в противоположном порядке. Окончательное произведение равно  $\alpha^{12} + \alpha^{11} - 115\alpha^{10} - 115\alpha^9 + 59\alpha^8 - 57\alpha^7 + 552\alpha^6 - 57\alpha^5 + \dots \equiv \alpha^{12} + \alpha^{11} + \alpha^{10} + \dots + \alpha + 1$ . 3.  $(X^2 - 4X + 1)(X^2 + 5X + 1) \pmod{19}$ ,  $(X^2 + 26X + 1) \times (X^2 - 25X + 1) \pmod{59}$ ,  $(X + 4)(X - 16)(X - 18)(X - 10) \pmod{41}$  все являются разложениями полинома  $X^4 + X^3 + X^2 + X + 1$ ;  $(X^2 + 3X + 1)(X^2 + 5X + 1)(X^2 + 6X + 1) \pmod{13}$  и  $(X + 13)(X + 5)(X - 7)(X + 4)(X + 6)(X + 9) \pmod{29}$  — разложения полинома  $X^6 + X^5 + \dots + 1$ . По модулю 2 полином  $X^{30} + X^{29} + \dots + 1$  является произведением 6 сомножителей  $X^5 + X^3 + 1$ ,  $X^5 + X^3 + X^2 + X + 1$ ,  $X^5 + X^4 + X^3 + X + 1$ ,  $X^5 + X^2 + 1$ ,  $X^5 + X^4 + X^3 + X^2 + 1$ ,  $X^5 + X^4 + X^2 + X + 1$ . 4. Векторное пространство над полем из  $p$  элементов имеет  $p^k$  элементов, где  $k$  — его размерность. 5.  $7\alpha^3 + 45\alpha^2 + 83\alpha + 90 = (38\theta_0 + 83)\alpha + (45 - 7\theta_0) = (\theta_1 - 5)(3\theta_0 - 8)[(2 + \theta_0)\alpha + 1]$ . 6. В полиноме  $P(\alpha)$  замените каждый коэффициент сравнимым с ним по модулю  $h(\alpha)$  целым числом и обозначьте результат  $Q_h(\alpha)$ . Тогда  $Q_h(\alpha) \equiv P(\alpha) \pmod{h(\alpha)}$  и легко показать, что  $Q_h(\alpha)$  обладает требуемыми свойствами.
- 4.9. 1.  $\Psi(\eta) = (1 - \eta_0)(1 - \eta_1)\eta_2(1 - \eta_3)\eta_4\eta_5$ . По модулю 2 имеем  $(1 - \eta_0)(1 - \eta_1)\eta_2 \equiv \eta_0 + \eta_3 + \eta_4 \equiv (1 - \eta_3)\eta_4\eta_5$ . Таким образом,  $\Psi(\eta) \equiv (\eta_0 + \eta_3 + \eta_4)^2 \equiv \eta_0 + \eta_3 + \eta_4$ . 2.  $\Psi(\eta) = (1 - \eta_0) \times (-1 - \eta_0)(1 - \eta_1)\eta_1(1 - \eta_2)\eta_2(-1 - \eta_3)\eta_3 \equiv \eta_0 - \eta_1 + \eta_3 \pmod{3}$ . 5. Коэффициенты инвариантны относительно  $\sigma$  и поэтому являются целыми числами;  $\lambda = 5$ :  $X^2 + X - 1$ ;  $\lambda = 7$ :  $X^2 + X + 2$  и  $X^3 + X^2 - 2X - 1$ ;  $\lambda = 11$ :  $X^2 + X + 3$  и  $X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$ ;  $\lambda = 13$ :  $X^2 + X - 3$ ,  $X^3 + X^2 - 4X + 1$ ,  $X^4 + X^3 + 2X^2 - 4X + 3$ ,  $X^6 + X^5 - 5X^4 - 4X^3 + 6X^2 + 3X - 1$ . По-видимому, самый легкий путь в этом убедиться заключается в том, чтобы выразить степени  $\eta_0^2, \eta_0^3, \dots, \eta_0^e$  через  $\eta_i$  и исключить остальные  $\eta_i$ . 6.  $(X - \eta_i - 1)(X - \eta_i - 2) \dots (X - \eta_i - p) \equiv (X - \eta_i)^p - (X - \eta_i) \equiv (X^p - X) - (\eta_i^p - \eta_i) \equiv X^p - X \equiv (X - 1)(X - 2) \dots (X - p) \pmod{p}$ . Перемножение этих полиномиальных сравнений для  $i = 1, 2, \dots, e$  дает  $\varphi(X - 1)\varphi(X - 2) \dots \varphi(X - p) \equiv (X - 1)^e(X - 2)^e \dots (X - p)^e \pmod{p}$ . Говорят, что  $j$  является корнем кратности точно  $k$  сравнения  $\varphi(X) \equiv 0 \pmod{p}$ , если  $\varphi(X) \equiv q(X)(X - j)^k \pmod{p}$  и  $q(j) \not\equiv 0 \pmod{p}$ , т. е.  $X - j$  не делит  $q(X)$  по модулю  $p$ . Тогда  $\varphi(X - 1)\varphi(X - 2) \dots \varphi(X - p) \equiv Q(X - 1)Q(X - 2) \dots Q(X - p)(X - 1)^t(X - 2)^t \dots (X - p)^t$ , где  $t$  — общее число корней сравнения  $\varphi(X) \equiv 0$ , подсчитанных с кратностями, а  $Q(X) \equiv 0$  не имеет корней. Если  $a(X)b(X) \equiv c(X)b(X) \pmod{p}$  и  $b(X) \not\equiv 0 \pmod{p}$ , то  $a(X) \equiv c(X) \pmod{p}$ . Таким образом,  $Q(X - 1)Q(X - 2) \dots Q(X - p) \equiv [(X - 1)(X - 2) \dots (X - p)]^{e-t}$ . Но сравнение  $Q(X) \equiv 0 \pmod{p}$  не имеет корней, и поэтому  $e = t$ , а это и требовалось показать. 7.  $\varphi(X) = X^2 - 1$ . 8. Вычислите  $\eta_0^2, \eta_0^3, \dots, \eta_0^e$  через  $\eta_i$ , запишите эти соотношения

как сравнения от  $u_i$  и используйте известное значение  $u_0$ . Это дает  $e - 1$  неоднородных линейных «уравнений» от  $e - 1$  неизвестных. Если определитель из коэффициентов отличен от нуля по модулю  $p$ , то этим однозначно определяются  $u_1, u_2, \dots, u_{e-1}$  по модулю  $p$ . Однако не очевидно, что если  $u_0, u_1, \dots, u_{e-1}$  удовлетворяют этим сравнениям, то они удовлетворяют *всем* сравнениям, вытекающим из соотношений между  $\eta_i$ . 9.  $p - \eta_i$  никогда не делится на  $p$  (поскольку его коэффициенты не сравнимы по модулю  $p$ ), кроме случая  $e = 1, f = \lambda - 1, \eta = -1$ , когда  $0 - \eta$  не делится на  $p$ . 11.  $\alpha^{-1} = \alpha^k \alpha$ , где  $k = (\lambda - 1)/2$ . Таким образом,  $\alpha^{-1}$  лежит в  $\eta_k$  и задача заключается в вычислении  $ef/2$  по модулю  $e$ . Если  $f$  четно, то  $ef/2 \equiv 0 \pmod{e}$ . В противном случае  $ef/2 \equiv e/2 \pmod{e}$ .

4.11. 1. См. доказательство второй теоремы из § 4.12. 2. Используйте способ из упр. 1.

4.12. 1. Пусть  $\varphi(\eta) = u_j - \eta_0$ . Если  $u_j$  встречается лишь однажды (по модулю  $p$ ) в списке  $u_1, u_2, \dots, u_e$ , то только один простой дивизор числа  $p$  делит  $\varphi(\eta)$ . Следовательно, то же самое верно для  $\varphi(\eta) + kp$  при всех  $k$ . Заметим, что  $(\varphi(\eta) + pk)(\sigma\varphi(\eta) + pk) \dots (\sigma^{e-1}\varphi(\eta) + pk) \equiv K + pkM \pmod{p^2}$ , где  $K = \prod \sigma^i \varphi(\eta)$  и  $M = \sum (K/\sigma^i \varphi(\eta))$ . Все слагаемые, кроме одного, в сумме  $M$  делятся на данный простой дивизор числа  $p$ . Таким образом,  $M \not\equiv 0 \pmod{p}$  и имеется точно одно по модулю  $p$  значение  $k$ , для которого  $(K/p) + kM \equiv 0 \pmod{p}$ . Значит, имеется точно одно значение  $k$ , для которого  $N(\varphi(\eta) + pk)$  делится на степень числа  $p$ , высшую, чем  $p^f$ . 2. По упр. 1 к § 4.9,  $\Psi(\eta) = \eta_0 + \eta_3 + \eta_4$ . Тогда  $\varphi(\eta) \equiv \eta_1 + \eta_2 + \eta_5$ . Либо  $\psi(\eta) = \varphi(\eta)$ , либо  $\psi(\eta) = \varphi(\eta) + 2$ . Вычисляя, получаем  $\varphi(\eta) \cdot \sigma^2 \varphi(\eta) \times \times \sigma^4 \varphi(\eta) = 9 - 5\theta_1$ . Таким образом,  $N\varphi(\eta) = 2^5 \cdot 163^5$  и простыми дивизорами числа 2 являются  $(2, \eta_1 + \eta_2 + \eta_5), (2, \eta_2 + \eta_3 + \eta_0), \dots, (2, \eta_0 + \eta_1 + \eta_4)$ . 3. Из-за  $N(1 - \alpha + \alpha^{-2})$  они могут быть записаны как  $(47, 1 - \alpha + \alpha^{-2})$  и его сопряженные. С другой стороны, поскольку  $N(\alpha - 4) = (4^{23} - 1)/(4 - 1) = 23\,456\,248\,059\,221$  не делится на  $47^2$ , они могут быть записаны как  $(47, \alpha - 4)$  и его сопряженные. 4. Разложение тогда и только тогда может быть записано в таком виде, когда по крайней мере одно из целых чисел  $u_1, u_2, \dots, u_e$  встречается с кратностью 1. Таким образом, это невозможно в упр. 2, возможно в упр. 3. 5. Пусть  $A = (p_1, \psi_1)^{\mu_1} \dots$ , как в тексте, и пусть  $n = p_1^{\mu_1} p_2^{\mu_2} \dots p_m^{\mu_m}$ . Тогда из сравнения по модулю  $n$  вытекает сравнение по модулю  $A$ , и имеется не больше  $n^{\lambda-1} < \infty$  классов сравнения по модулю  $n$ . 6. См. упр. 2 к § 4.11.

4.13. 1. (iii) Если  $a$  и  $b$  — круговые целые, для которых  $ab \in \mathcal{Y}$ , то  $a \in \mathcal{Y}$  или  $b \in \mathcal{Y}$ . 2.  $\sum b_i g_i$  всегда лежит в  $\mathcal{Y}$ . Обратно, если  $x \in \mathcal{Y}$ , то  $x \equiv g_i \pmod{g_1}$  для некоторого  $g_i$  и  $x = g_i + b_1 g_1$  для некоторого  $b_1$ . 3.  $\mathcal{Y}$  соответствует наибольшему общему делителю элементов  $g_1, g_2, \dots, g_n$ , кроме случая  $\mathcal{Y} = \{0\}$ .

4.14. 1. Если  $A$  — степень простого дивизора, скажем  $A = P^v$ , и  $\sigma A$  делит  $g(\alpha)$ , то  $p^v$  делит  $g(\alpha) \cdot \sigma \Psi(\eta)^v$ , откуда вытекает, что  $p^v$  делит  $\sigma^{-1} g(\alpha) \times \times \Psi(\eta)^v$  и, стало быть,  $A$  делит  $\sigma^{-1} g(\alpha)$ . Если  $A, B$  взаимно просты и  $\sigma(AB) = \sigma(A)\sigma(B)$  делит  $g(\alpha)$ , то  $\sigma(A)$  и  $\sigma(B)$  делят  $g(\alpha)$ ,  $A$  и  $B$  делят  $\sigma^{-1} g(\alpha)$  и, следовательно,  $AB$  делит  $\sigma^{-1} g(\alpha)$ . Это показывает, что для любого  $A$  из  $g(\alpha) \equiv 0 \pmod{\sigma A}$  вытекает  $\sigma^{-1} g(\alpha) \equiv 0 \pmod{A}$ . Тогда  $g(\alpha) \equiv 0 \pmod{\sigma^i A}$  влечет за собой  $\sigma^{-1} g(\alpha) \equiv 0 \pmod{\sigma^{i-1} A}, \dots, \sigma^{-i} g(\alpha) \equiv 0 \pmod{A}$ . Обратно, из  $\sigma^{-i} g(\alpha) \equiv 0 \pmod{\sigma^{\lambda-1-i}(\sigma^i A)}$  вытекает  $g(\alpha) = \sigma^{-(\lambda-1)+i} \cdot \sigma^{-i} g(\alpha) \equiv$



$\equiv 0 \pmod{\sigma^i A}$ . Таким образом,  $(g_1 - g_2) \equiv 0 \pmod{\sigma^i A}$ , равносильно условию  $\sigma^{-i}(g_1 - g_2) \equiv 0 \pmod{A}$ , что и требовалось доказать.

2. Норма произведения есть произведение норм. Для простых дивизоров доказательство несложно. 3. Пусть  $AC$  — дивизор элемента  $g_n$ . Тогда  $B$  и  $C$  взаимно просты. Запишите  $A = A' A_B A_C$ , где  $A_B$  содержит все простые делители дивизора  $A$ , встречающиеся в  $B$ , а  $A_C$  — все простые делители, встречающиеся в  $C$ . Найдите такое  $y$ , чтобы  $y \equiv 1 \pmod{A_B B}$  и  $y \equiv 0 \pmod{A_C C}$ . Тогда  $\varphi y \equiv \varphi \pmod{A_B B}$  и  $\varphi y \equiv 0 \equiv \varphi \pmod{A' A_C}$ , так что  $\varphi y = \varphi$  по модулю  $AB$ . Аналогично,  $\varphi y \equiv 0 \pmod{AC}$ ,  $\varphi y = b_n g_n$ .

4.15. 2. Предположим, что  $P = (p, \psi)$  не является дивизором никакого кругового целого. Если  $\psi = \psi_1 \psi_2$ , то либо  $P = (p, \psi_1)$ , либо  $P = (p, \psi_2)$ . Поэтому предположим, что  $\psi$  неразложимо. Пусть  $N\psi = p^f p_1^{v_1} \dots p_n^{v_n}$ . Запишем  $p, p_1, \dots, p_n$  как произведения неразложимых. Тогда  $N\psi$  представляется в виде произведения неразложимых двумя существенно различными способами.

5.2. 1.  $\lambda = 31$ :  $(a + b\theta_0)(a + b\theta_1) = a^2 - ab + 8b^2$ . Даже очень короткая таблица дает  $(1 + \theta_0) = (2, 1)^3$ ,  $(2 + \theta_0) = (2, 0)(5, -2)$ ,  $(3 + \theta_0) = (2, 1)(7, -3)$ . Таким образом,  $(2, 1) \sim (5, -2) \sim (7, 2)$  и  $(2, 1)^3 \sim I$ . Как и раньше,  $(2, 1) \not\sim I$  и, следовательно,  $(2, 1)^2 \not\sim I$ . Поскольку  $1/4 p^2 + 1/2 p + 8 < p^2$  при  $p \geq 5$ , каждый дивизор является произведением простых дивизоров чисел 2 или 3. Но показатель числа 3 по модулю 31 есть 30, поэтому 3 просто. Следовательно,  $I, (2, 1), (2, 1)^2 \sim (2, 0)$  — система представителей.  $\lambda = 39$ :  $(a + b\theta_0)(a + b\theta_1) = a^2 - ab + 10b^2$ . Опять подходят лишь  $p = 2, 3$ .  $(3 + \theta_1) = (2, 1)^4$ ,  $(2 + \theta_1) = (2, 0)^2(3, 1)$ . Таким образом,  $(2, 1)^2 \sim (3, 1)$ . Так как ни  $(2, 1)$ , ни  $(3, 1)$  не эквивалентны  $I$ , то систему представителей образуют  $I, (2, 1), (2, 1)^2 \sim (3, 0)$  и  $(2, 1)^3 \sim (2, 0)$ .  $\lambda = 43$ :  $a^2 - ab + 11b^2$ . Снова подходят лишь  $p = 2, 3$ . Короткая таблица значений дает простые значения и показывает отсутствие простых дивизоров чисел 2 и 3. Действительно, 2 имеет показатель 14, а 3 — показатель 42, так что  $e$  является нечетным в обоих случаях, и дивизоров вида  $(2, u)$  и  $(3, u)$  нет. Итак, все дивизоры главные, и  $I$  — система представителей.

5.3. 1. (1) Если  $f(\alpha)$  имеет дивизор  $A$  и  $g(\alpha)$  имеет дивизор  $B$ , то  $f(\alpha)g(\alpha)$  имеет дивизор  $AB$ . (2) Если  $f(\alpha)$  имеет дивизор  $A$  и  $h(\alpha)$  имеет дивизор  $AB$ , то  $f(\alpha)$  делит  $h(\alpha)$  и частное имеет дивизор  $B$ . (3) Если  $A \sim I$ , то  $A$  — главный, поскольку таковым является  $I$  (замените  $A$  на  $I$  в  $A$ ). Если  $A$  — главный, то на основании (1) и (2) дивизор  $C$  тогда и только тогда является главным, когда таковым является  $AC$ ; значит,  $A \sim I$ . (4) Если  $AC \sim BC \sim I$  и  $AD \sim I$ , то  $(BD)(AC) = (AD)(BC) \sim I$  по (1), следовательно,  $BD \sim I$  по определению эквивалентности  $AC \sim I$ . По симметрии, из  $BD \sim I$  следует  $AD \sim I$ . Значит,  $A \sim B$ . Теперь допустим, что  $A \sim B$ . На основании (7) имеется такой дивизор  $C$ , что  $AC \sim I$ . Тогда  $BC \sim I$  по определению. Утверждения (5) и (6) получаются непосредственно. (7)  $N(A)$  — дивизор некоторого целого числа; значит, дополнение  $B$  дивизора  $A$  до  $N(A)$  обладает требуемыми свойствами. (8) Пусть  $C$  такой, что  $AC \sim I$ , и положим  $M = BC$ ,  $N = AC$ . 2. См. упр. 2 к § 4.15. 3. При  $g(\alpha) = a_1\alpha + a_2\alpha^2 + \dots + a_{\lambda-1}\alpha^{\lambda-1}$  имеем  $g(\alpha)g(\alpha^{-1}) = a_1^2 + a_1a_2\alpha^{-1} + a_1a_3\alpha^{-2} + \dots + a_2a_1\alpha + a_2^2 + a_2a_3\alpha^{-1} + \dots$ . Тогда сумма  $\lambda - 1$  сопряженных равна  $(\lambda - 1)(a_1^2 + a_2^2 + \dots + a_{\lambda-1}^2) - (a_1a_2 + a_1a_3 + \dots + a_2a_1 + a_2a_3 + \dots) = \lambda \sum a_i^2 - \left(\sum a_i\right)^2$ . Если  $|a_i| \leq c$  во всех случаях, то  $Ng(\alpha)$  является произведением  $(\lambda - 1)/2$  положительных веществен-



ных сомножителей, среднее арифметическое которых не превосходит  $[\lambda(\lambda-1)c^2-0]/(\lambda-1) = \lambda c^2$ . Так как их среднее геометрическое  $(Ng(\alpha))^{2/(\lambda-1)} \leq \lambda c^2$ , то отсюда следует результат.

5.5. 1. Из  $\alpha \equiv 1$  следует  $g(\alpha) \equiv g(1) =$  целое число по модулю  $\alpha - 1$ . Если  $g(\alpha) \equiv a_0 \pmod{\alpha - 1}$ , то пусть  $h(\alpha) = [g(\alpha) - a_0]/(\alpha - 1)$ . Тогда  $h(\alpha) \equiv a_1 \pmod{\alpha - 1}$  и  $g(\alpha) \equiv a_0 + a_1(\alpha - 1) \pmod{(\alpha - 1)^2}$ . Если  $[g(\alpha) - a_0 - a_1(\alpha - 1)]/(\alpha - 1)^2 \equiv a_2 \pmod{\alpha - 1}$ , то  $g(\alpha) \equiv a_0 + a_1(\alpha - 1) + a_2(\alpha - 1)^2 \pmod{(\alpha - 1)^3}$ , и т. д. Если  $a_0 + a_1(\alpha - 1) + \dots + a_{\lambda-2}(\alpha - 1)^{\lambda-2} \equiv b_0 + b_1(\alpha - 1) + \dots + b_{\lambda-2}(\alpha - 1)^{\lambda-2} \pmod{(\alpha - 1)^{\lambda-1}}$ , то  $c_0 + c_1(\alpha - 1) + \dots \equiv 0 \pmod{(\alpha - 1)^{\lambda-1}}$ , где  $c_i = a_i - b_i$ . Тогда  $c_0 \equiv 0 \pmod{\alpha - 1}$ , откуда  $c_0 \equiv 0 \pmod{\lambda}$ ,  $c_0 \equiv 0 \pmod{(\alpha - 1)^{\lambda-1}}$ . Далее,  $c_1(\alpha - 1) \equiv 0 \pmod{(\alpha - 1)^2}$ ,  $(\alpha - 1) \mid c_1$ ,  $c_1 \equiv 0 \pmod{(\alpha - 1)^{\lambda-1}}$ . Далее,  $c_2 \equiv 0 \pmod{(\alpha - 1)^{\lambda-1}}$  и т. д. 2. Исключите  $x$  из сравнений  $(\alpha^k - \alpha^{-k})x \equiv (\alpha^{1-k} - \alpha^{k-1})y$ ,  $(\alpha^{2k} - \alpha^{-2k})x \equiv (\alpha^{2-2k} - \alpha^{2k-2}) \times \times y \pmod{\lambda}$ , умножив первое на  $\alpha^k + \alpha^{-k}$  и вычтя его из второго. Воспользуйтесь тем фактом, что  $(\alpha - 1)^2 \mid (\alpha^\mu - \alpha^\nu)$  только тогда, когда  $\alpha^\mu = \alpha^\nu$ . Если  $(\alpha - \alpha^{-1})x \equiv 0 \pmod{\lambda}$ , то  $a \equiv 0 \pmod{\lambda}$ . Если  $(\alpha - \alpha^{-1})x \equiv (\alpha - \alpha^{-1})y \pmod{\lambda}$ , то  $a \equiv b \pmod{\lambda}$ .

5.6. 1. Вкратце вычисления выглядят так:  $1 + 3 = 4 + 5 = 9 + 7 = 16 + 9 = 25 + 11 = 36 + 13 = 49 + 15 = 64 + 17 = 81 \equiv 2 + 19 = 21 + 21 = 42 + 23 = 65 + 25 = 90 \equiv 11 + 27 = 38 + 29 = 67 + 31 = 98 \equiv 19 + 33 = 52 + 35 = 87 \equiv 8 + 37 = 45 + 39 = 84 \equiv 5 + 41 = 46 + 43 = 89 \equiv 10 + 45 = 55 + 47 = 102 \equiv 23 + 49 = 72 \equiv -7 + 51 = 44 + 53 = 97 \equiv 18 + 55 = 73 = -6 + 57 = 51 + 59 = 110 \equiv 31$ . Так как  $59 = 29 + 30$ , то это дает  $31 \equiv 30^2 \pmod{79}$ . 2. Неравенство, ограничивающее  $y$ , получается из  $0 < x^2 < (m/2)^2$ . Когда  $A = 31$ ,  $m = 79$ , значения  $y$  лежат в пределах  $0 \leq y \leq 19$ . Из того что  $31 + 79y \equiv 0$  или  $1 \pmod{3}$ ,  $1 + y \not\equiv 2 \pmod{3}$ , следует, что  $y \not\equiv 1 \pmod{3}$ . Это исключает возможности 1, 4, 7, 10, 13, 16, 19. Аналогично,  $31 + 79y \equiv 0$  или  $1 \pmod{4}$  исключает значения  $y \equiv 0$  или  $1 \pmod{4}$ ;  $31 + 79y \equiv 0$  или  $1$  или  $4 \pmod{5}$  исключает  $y \equiv -1$  или  $-2 \pmod{5}$ . Остаются только  $y = 2, 6, 11, 15$ ;  $31 + 79y \equiv 0, 1$  или  $4 \pmod{8}$  исключает значение 2;  $31 + 79y \equiv 0, 1, 2$  или  $4 \pmod{7}$  исключает значение 15. Так как  $6 \cdot 79 + 31 = 505$  не является квадратом, то ответ должен быть  $y = 11$ . И действительно,  $31 + 79 \cdot 11 = 900 = 30^2$ . 3.  $\binom{22}{97} = \binom{2}{97} \binom{11}{97} = \binom{2}{1} \binom{97}{11} = \binom{9}{11} = \binom{3}{11}^2 = +1$ ;  $y = 0, 1, \dots$  или 24. Модуль  $E = 8$  дает  $y \equiv 2, 3$  или  $6 \pmod{8}$ . Модуль  $E = 9$  дает  $y \equiv 0, 2, 3, 6 \pmod{9}$ ;  $E = 5$  дает  $y \equiv 1, 2, 4 \pmod{5}$ . Это приводит к значениям  $y = 2, 6$  или  $11$ . 4.  $\binom{79}{101} = \binom{101}{79} = \binom{22}{79} = \binom{2}{79} \binom{11}{79} = \binom{2}{7} [-\binom{79}{11}] = -\binom{2}{11} = -\binom{2}{3} = +1$ ;  $\binom{97}{139} = \binom{139}{97} = \binom{42}{97} = \binom{2}{97} \binom{3}{97} \binom{7}{97} = \binom{2}{1} \binom{97}{3} \binom{97}{7} = \binom{1}{3} \binom{6}{7} = \binom{6}{7} = -1$ ;  $\binom{91}{139} = \binom{7}{139} \binom{13}{139} = -\binom{139}{7} \binom{139}{13} = -\binom{6}{7} \binom{9}{13} = -\binom{6}{7} = +1$ . 6.  $\binom{2}{p} = \binom{-1}{p} \binom{-2}{p}$  и  $\binom{-2}{p}$  равен  $+1$  для  $p \equiv 1$  или  $3 \pmod{8}$  и равен  $-1$  для  $p \equiv 5$  или  $7 \pmod{8}$ . 8. Докажите отдельно критерий Эйлера, как в упр. 7. Выведите правило (1). Тогда если  $p \equiv 1 \pmod{4}$ , то  $\binom{p}{q} = \binom{q}{p}$ . Если  $p \equiv 3$  и  $q \equiv 1 \pmod{4}$ , то  $\binom{q}{p} = \binom{p}{q} = \binom{-1}{q} \binom{p}{q}$ . Если  $p \equiv q \equiv$

$\equiv 3 \pmod{4}$ , то  $\binom{q}{p} = -\binom{p}{q} = \binom{-1}{q} \binom{p}{q}$ . 9. Как  $p-1$ , так и  $q-1$  четны. Если  $p \equiv 1$  или  $q \equiv 1 \pmod{4}$ , то  $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$  четно. Если как  $p \equiv 3$ , так и  $q \equiv 3 \pmod{4}$ , то  $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$  нечетно. 10. Из первого сравнения вытекает  $24u^2 - 16u \equiv 56$ ,  $u^2 - 16u + 64 - 64 \equiv 10$ ,  $(u-8)^2 \equiv 5 \pmod{23}$ . Так как  $\binom{5}{23} = \binom{23}{5} = \binom{3}{5} = -1$ , то это невозможно. Из второго вытекает  $35u^2 + 30u \equiv 10$ ,  $-2u^2 + 30u \equiv 10$ ,  $u^2 - 15u \equiv -5$ ,  $u^2 + 22u + 121 \equiv 116$ ,  $(u+11)^2 \equiv 5 \pmod{37}$ . Так как  $\binom{5}{37} = \binom{37}{5} = \binom{2}{5} = -1$ , то это также невозможно. 11. Если сравнение  $x^2 \equiv B \pmod{p}$  имеет решение, то  $B^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$ . Следовательно,  $B^{(p+1)/2} \equiv B \pmod{p}$  и квадрат числа  $x \equiv B^{(p+1)/4}$  равен  $B \pmod{p}$ . Вычисление значения  $31^{20}$  по модулю 79 просто:  $31^2 \equiv 13$ ,  $31^4 \equiv 13^2 \equiv 11$ ,  $31^8 \equiv 121 \equiv 42$ ,  $31^{16} \equiv 42^2 \equiv 26$ ,  $31^{20} \equiv 11 \cdot 26 \equiv 49 \equiv -30$ .

6.3. 1. Если произведение записано в виде произведения по  $p \equiv 1 \pmod{\lambda}$ , умноженного на произведение по  $p \not\equiv 1 \pmod{\lambda}$ , то второй сомножитель меньше  $\prod (1 - p^{-2s})^{-(\lambda-1)} < \prod (1 - p^{-2})^{1-\lambda} = \zeta(2)^{\lambda-1} < \infty$  и больше 1. Первый сомножитель представляет собой произведение по всем  $p \equiv 1 \pmod{\lambda}$  выражений  $(1 - p^{-s})^{-(\lambda-1)}$ . Его логарифм равен  $(\lambda-1) \sum (p^{-s} + \frac{1}{2}p^{-2s} + \frac{1}{3}p^{-3s} + \dots) = (\lambda-1) \sum p^{-s} +$  конечная величина, где сумма берется по  $p \equiv 1 \pmod{\lambda}$ , поскольку  $\log(1-x)^{-1} - x \leq x^2/2$  для  $0 \leq x \leq 1/2$ . 2.  $1000 < \zeta(s) < 1 + 1000$ . 3. Как и в упр. 1,  $\sum n^{-s} = \sum p^{-s} +$  конечная величина. Так как  $p^{-s} < p^{-1}$ , то из  $\sum p^{-1} < \infty$  вытекало бы, что  $\sum p^{-s}$  ограничена при  $s \downarrow 1$ , и, стало быть,  $\sum n^{-s}$  также ограничена при  $s \downarrow 1$ .

6.4. 1. Степени числа  $\beta$  являются различными корнями полинома  $X^n - 1$ , так что  $X^n - 1 = (X - \beta)(X - \beta^2) \dots (X - \beta^n)$ . Положите  $X = x/y$  и умножьте на  $y^n$ . Если  $\beta$  является корнем  $\mu$ -й степени при некотором  $\mu$ , то  $n = \mu\nu$  и произведение равно  $(x^\mu - y^\mu)^\nu$ . 2. Предположим, что  $p \equiv \gamma^j \pmod{\lambda}$ . Тогда  $\beta^j$  — примитивный корень  $f$ -й степени из 1 и на основании упр. 1  $\prod_k (1 - \beta^{jk} p^{-s}) = (1^f - (p^{-s})^f)^e = \prod (1 - N(P))^{-s}$ , где  $P$  пробегает простые дивизоры числа  $p$ . Перестановка сомножителей в произведении допустима из-за абсолютной сходимости. 3. Значения характера  $\chi_0$  равны 1, за исключением значений аргумента, кратных числу 13, при которых  $\chi_0 = 0$ . Значение  $\chi_6(n)$  равно 0 для  $n \equiv 0 \pmod{13}$ , равно 1 для  $n \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$  и равно  $-1$  для остальных  $n$ . Первые 10 ненулевых членов соответствуют значениям  $n = 1, 2, 3, 4, 6, 8, 9, 12, 16, 18$ . 4. Из  $\chi(2)^3 = 0$  вытекает  $\chi(n) = 0$  для четных  $n$ . Из  $\chi(3)^2 = 1$  и  $\chi(5)^2 = 1$  вытекает  $\chi(3) = \pm 1$ ,  $\chi(5) = \pm 1$ . Из  $\chi(7) = \chi(3)\chi(5)$  вытекает, что значения  $\chi(3)$  и  $\chi(5)$  определяют  $\chi$ .

6.5. 1. Из  $(1 - \theta_0)(1 - \theta_1) = 1$  вытекает  $\log(1 - \theta_0) = -\log(1 - \theta_1)$ . 2. На основании (8)  $L(1, \chi_3) = (i\pi m_3/\lambda)(1 - 3 + 2 - 6 + 4 - 5)$ , где  $m_3 = (\alpha - \alpha^3 + \alpha^2 - \alpha^6 + \alpha^4 - \alpha^5)/7 = (\theta_0 - \theta_1)/7$ . Из геометрических соображений,  $\theta_0$  лежит в верхней полуплоскости, а  $\theta_1$  — в нижней. Из  $(\theta_0 - \theta_1)^2 = -7$  получаем  $\theta_0 - \theta_1 = i\sqrt{7}$  и  $L(1, \chi_3) = \pi/\sqrt{7} = 1,1874 \dots$ . 3.  $\sigma^\mu \alpha$  равно  $\alpha$  в степени  $\gamma^\mu$ . Так как  $(\gamma^\mu)^2 = \gamma^{\lambda-1} \equiv 1 \pmod{\lambda}$  и  $\gamma^\mu \not\equiv 1 \pmod{\lambda}$ , то  $\gamma^\mu \equiv -1 \pmod{\lambda}$ . 4.  $\lambda =$

$= 3: L(1, \chi_1) = i\pi (\omega - \omega^2) (1 - 2)/3^2 = \pi/3 \sqrt{3}; \lambda = 5: L(1, \chi_1) = i\pi (\alpha + i\alpha^2 - \alpha^4 - i\alpha^3) (1 - 2i - 4 + 3i)/5^2 = (2\pi \sin(2\pi/5) + 2\pi i \sin(4\pi/5)) (3 - i)/25; L(1, \chi_2) = (\sqrt{5}/5) \log((3 + \sqrt{5})/2); L(1, \chi_3) = \overline{L(1, \chi_1)}; \lambda = 7: L(1, \chi_3) = \pi/\sqrt{7}; L(1, \chi_1) = i\pi (\alpha + \beta\alpha^3 + \beta^2\alpha^2 + \beta^3\alpha^6 + \beta^4\alpha^4 + \beta^5\alpha^5) (\beta^{-1} + 3\beta^{-2} + 2\beta^{-3} + 6\beta^{-4} + 4\beta^{-5} + 5\beta^{-6})/49, \text{ где } \beta = \exp(2\pi i/6), \alpha = \exp(2\pi i/7); L(1, \chi_5) = \overline{L(1, \chi_1)}; L(1, \chi_2) = -2(\alpha + \omega\alpha^3 + \omega^2\alpha^2 + \alpha^6 + \omega\alpha^4 + \omega^2\alpha^5) (\log|1 - \alpha| + \omega^{-1} \log|1 - \alpha^3| + \omega^{-2} \log|1 - \alpha^2|)/7, \text{ где } \omega = \exp(2\pi i/3); L(1, \chi_4) = \overline{L(1, \chi_2)}.$

6.9. 1.  $\theta^j = (-1)^j [a_{j-1} - a_j \theta]$ , где последовательность  $\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots$  определяется равенствами  $a_0 = 0, a_1 = 1, a_{i+1} = a_i + a_{i-1}$ . Ясно, что тогда  $\theta^j \neq \pm \theta^i$ , кроме случая, когда  $i = j$  и стоит знак  $+$ . Пусть  $a + b\theta$  — единица. Если  $a + b\theta$  имеет норму  $-1$ , то  $(a + b\theta)\theta$  имеет норму  $1$ . Если  $b$  нечетно, то коэффициент при  $\theta$  либо в  $(a + b\theta)\theta$ , либо в  $(a + b\theta)\theta^2$  четный. Следовательно, достаточно показать, что если  $N(a + b\theta) = 1$  и  $b$  четно, то  $a + b\theta = \pm \theta^j$ . Так как равенство  $N(a + 2c\theta) = N((a - c) + c(\theta_0 - \theta_1)) = (a - c)^2 - 5c^2$  дает решение уравнения Пелля, то единица имеет вид  $(a - c) + c\sqrt{5} = \pm (9 + 4\sqrt{5})^j$ , где  $\theta_0 - \theta_1 = \sqrt{5}$ . Так как  $9 + 4\sqrt{5} = 13 + 8\theta_0 = \theta^6$ , то это показывает, что  $a + b\theta = \pm \theta^6 j$ . 4.  $1 + 2\eta_0 = -\eta_0^2 \eta_1^{-1}$ . 6.  $1 + \rho^{i-j} + \rho^{2i-2j} + \dots + \rho^{-i+j}$  равно  $0$ , если  $i \not\equiv j \pmod{n}$ , и равно  $1$ , если  $i \equiv j \pmod{n}$ . 8. Пусть  $e_0 = (1 - \sigma^2 \alpha)(1 - \sigma \alpha)^{-1}$  для некоторого фиксированного  $\sigma$ , и пусть  $e_{i+1} = \sigma e_i$ . Соображения, приведенные в тексте, показывают, что  $\log|e_{j+\mu}| = \log|e_j|$  (здесь  $\mu = 8$ ) и что система уравнений

$$\log|\sigma^i E(\alpha)| = \sum_{j=0}^{\mu-1} r_j \log|e_{j+i}| \text{ неявно определяет неизвестные } r_j$$

как функции единицы  $E(\alpha)$ . (В случае  $\lambda = 7$ , приведенном в тексте,  $\eta_0 = \alpha^{-1}e_0$ ,  $\log|\eta_i| = \log|e_i|$ .) При  $\lambda = 17$  выберите  $\sigma: \alpha \mapsto \alpha^3$ . Тогда  $\eta_0 = \alpha^{-1}(1 - \alpha^4)(1 - \alpha^2)^{-1} = \alpha^{-1}(1 - \sigma^{12}\alpha)(1 - \sigma^{14}\alpha)^{-1} = \alpha^{-1}e_{11}^{-1}e_{12}^{-1}$ ,  $\log|\eta_0| = -\log|e_3| - \log|e_4|$ , т. е. для  $E(\alpha) = \eta_0$  получаем  $r_3 = r_4 = -1$ , а остальные  $r_j$  равны  $0$ . Если  $E(\alpha)$  — произведение степеней периодов  $\eta_j$ , то сумма соответствующих  $r_j$  четна. Следовательно,  $e_0$  не является произведением степеней периодов  $\eta_j$ . Так как каждая единица вида (4) есть произведение единиц  $e_i$ , то достаточно выразить единицы  $e_i$  (на самом деле единицу  $e_0$ ) через периоды  $\eta_j$ . Если  $2$  — примитивный корень по модулю  $\lambda$ , то  $e_0 = (1 - \alpha^4)(1 - \alpha^2)^{-1} = 1 + \alpha^2 = \alpha^{-1}\eta_0$ , а если примитивным корнем по модулю  $\lambda$  является  $-2$ , то (как в случае  $\lambda = 7$ )  $e_0 = (1 - \alpha^4) \times (1 - \alpha^{-2})^{-1} = -\alpha^4(1 - \alpha^{-4})(1 - \alpha^{-2})^{-1} = -\alpha^3\eta_0$ .

6.10. 2. Если  $\Phi(e_1) - \Phi(e_2)$  имеет целые компоненты, то  $e_1$  эквивалентна произведению  $e_3 e_2$ , где  $e_3$  — вещественная единица, для которой  $\Phi(e_3)$  имеет нулевые компоненты. Так как  $Le_3 = 0$ ,  $e_3 = \pm 1$ .

6.14. 1. При помощи прямого вычисления получаем  $P = -1, 2 \cdot 5, -2^2 \cdot 7^2, -2^4 \cdot 11^4, 2^5 \cdot 13^5$  для  $\lambda = 3, 5, 7, 11, 13$  соответственно.

6.15. 1. Докажите, что для каждого  $k$  существует  $k$ -й круговой полином, т. е. полином  $\Phi_k$  с целыми коэффициентами и со старшим коэффициентом  $1$ , корни которого в точности совпадают с примитивными корнями  $k$ -й степени из единицы. Это делается делением полинома  $X^k - 1$  на полиномы  $\Phi_j$  для всех собственных делителей  $j$  числа  $k$ . Иными словами,  $\Phi_k(X) = (X - \beta_1)(X - \beta_2) \dots (X - \beta_{\varphi(k)})$ . Для каждого фиксированного  $j$  сумма  $\sum \beta_i^j$  есть целое число. Это можно доказать,

либо заметив, что  $\beta_i^j$  пробегает все примитивные корни  $(k/d)$ -й степени, где  $d = \text{н. о. д. } (k, j)$ , причем каждый из них появляется одинаковое число раз, либо воспользовавшись общей теоремой о том, что каждый симметрический полином является полиномом от основных симметрических полиномов. Таким образом,  $g(\beta_1) + g(\beta_2) + \dots + g(\beta_{\varphi(n)})$  есть, с одной стороны, целое число, а с другой стороны, число  $\varphi(n) g(\beta_1)$ . Значит,  $g(\beta_1) = r$ , где  $r$  — рациональное число (со знаменателем, который делит  $\varphi(n)$ ). Разделим с остатком полином  $\psi(X) = g(X) - r$  на  $\Phi_n(X)$ , положив  $\psi(X) = q(X)\Phi_n(X) + r(X)$ . Тогда  $r(X)$  имеет меньшую степень, чем  $\Phi_n(X)$ , и  $r(\beta_i) = 0$  для всех  $\beta_i$ . Значит,  $r(X) = 0$  и  $g(X) - r = q(X)\Phi_n(X)$ , откуда сле-

дует, что  $r$  — целое число. 3. Пусть  $I_k(x) = \int_x^{x+1} t^k dt$ . Тогда  $I_k(x)$  —

полином степени  $k$  со старшим коэффициентом 1. Два полинома принимают равные значения при всех  $x$  только тогда, когда они тождественны. Требуемое равенство равносильно системе равенств вида  $a_N = \text{известная величина}$ ,  $a_{N-1} + qa_N = \text{известная величина}$ ,  $a_{N-2} + ra_{N-1} + sa_N = \text{известная величина}$ ,  $\dots$ . Все эти известные величины равны 0, кроме одной, начинающейся с  $a_n$ , которая равна 1. Тогда из этих равенств следует, что  $N \geq n$ . Обратно, если  $N \geq n$ , то имеется один и только один набор коэффициентов  $a_i$ , удовлетворяющий этим равенствам (поскольку система треугольная). 4. Достаточно доказать, что обе части равенства имеют равные производные. В обоих

случаях производная равна  $\sum_{k=0}^{n-1} n! B_k x^{n-1-k} / k! (n-k-1)!$ ; в первом

случае это получается прямым вычислением, а во втором — по индук-

ции. 5.  $(-x)^n = \int_{-x}^{-x+1} B_n(t) dt = \int_{x+1}^x B_n(1-u) d(1-u) = \int_x^{x+1} B_n(1-u) \times$

$\times du$ ,  $x^n = \int_x^{x+1} (-1)^n B_n(1-t) dt$ . Таким образом,  $B_{2n+1}(1/2) =$

$= (-1) B_{2n+1}(1/2)$ ,  $B_{2n+1}(1/2) = 0$ . Тогда равенство  $B_{2n+1} = 0$  для  $n > 0$  следует из  $B_{2n+1}(1/2) - B_{2n+1} = 2^{-2n} \cdot (1 - 2^{2n+1}) B_{2n+1}$ .

6.  $B_3(t) = t(t-1/2)(t-1)$  равно нулю при 0, 1/2, 1, положительно между 0 и 1/2 и отрицательно между 1/2 и 1;  $B_5(t)$  равно 0 при 0, 1/2, 1. Оно не может иметь других нулей при  $0 \leq t \leq 1$ , поскольку иначе его производная  $5B_4(t)$  имела бы 3 нуля, а  $20B_3(t)$  — два нуля в этом интервале. Аналогично, единственными нулями полинома  $B_{2n+1}(t)$  на интервале  $0 \leq t \leq 1$  являются 0, 1/2, 1. Значит, полином  $B_{2n}(t)$  монотонен на интервале  $0 \leq t \leq 1/2$  и имеет там точно один нуль. Если  $B_{2n}(0) > 0$ , то  $B_{2n}(t)$  убывает и  $B_{2n-1}(t) < 0$  для  $0 < t < 1/2$ ; этот полином убывает от 0 до минимального значения, а затем возрастает до 0 в точке 1/2, так что его производная отрицательна в 0 и  $B_{2n-2} < 0$ .

Аналогично, если  $B_{2n} < 0$ , то  $B_{2n-2} > 0$ . 7.  $B_n(x) - B_n = n[1 + 2^{n-1} + 3^{n-1} + \dots + (x-1)^{n-1}] = \text{целое число}$ . 8.  $\psi(x) = x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{13} + x^{15} + x^{16} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{26} + x^{30} + x^{35} + x^{36}$ . Используя последовательность степеней числа 2, а именно 2, 4, 8, 16, —5, —10,  $\dots$ , 14, —9, —18, 1, мы находим  $\psi(2) \equiv -10 + 17 - 6 - 12 + 13 + 15 - 14 + 9 - 2 - 4 - 8 - 16 + 5 + 3 + 11 + 7 - 18 + 1 = -9$ . Для нахождения  $\psi(2^n)$  составляем последовательность степеней числа  $2^n$ . Если  $n = 31$ , то  $2^n \equiv -15$ , и мы находим  $\psi(2^{31}) \equiv -10 + 2 + 6 - 16 + 18 + 17 + 14 + 12 + 15 - 3 + 8 - 9 - 13 - 7 + 11 - 4 - 5 + 1 \equiv 0 \pmod{37}$ . 9. Хорошим контролем построения треуголь-

ника Паскаля по модулю 13 служит тот факт, что строка, соответствующая показателю 12, имеет вид  $1, -1, 1, -1, \dots, -1, 1$ . Решая сравнения  $B_0 = 1, B_0 + 2B_1 \equiv 0, B_0 + 3B_1 + 3B_2 \equiv 0, B_0 + 5B_1 - 3B_2 - 3B_3 + 5B_4 \equiv 0, \dots$ , без труда найдем  $B_0 \equiv 1, B_1 \equiv 6, B_2 \equiv -2, B_4 \equiv 3, B_6 \equiv -4, B_8 \equiv 3, B_{10} \equiv 5$ . (Конечно,  $B_{2n+1} \equiv 0$  для  $n > 0$ .) Прямой подсчет значения  $B_{10}$  (7) показывает, что оно  $\equiv -4 \pmod{13}$ . Таким же образом  $B_{10}(1/2) = B_{10} + 2^{-9}(1 - 2^{10})B_{10} \equiv -4$ .

- 6.16. 1.  $\psi(\gamma^n) \equiv (\gamma_{n+1} - 1) B_{n+1} (n+1)^{-1} \pmod{\lambda}$  для  $0 < n \leq \lambda - 3$ .  
2. Если  $\lambda = 13$ , то  $\psi(2^n) \equiv -3, 0, -5, 0, -3, 0, 3, 0, -2, 0, 3, 6$  для  $n = 1, 2, \dots, 12$ .

- 6.17. 1. Если  $h$  — порядок группы  $G$ , то элемент  $a^h$  — единица при любом  $a$  из  $G$ . Если  $\lambda \nmid h$ , то  $m\lambda = nh + 1$  и  $a = a \cdot a^{hn} = a^{m\lambda}$ . 2. Пусть  $e_2(\alpha) = \alpha^m E(\alpha)$ , где  $E(\alpha)$  — вещественная единица. Тогда условие  $\pm \alpha^k = e_2(\alpha)^\lambda = \alpha^{m\lambda} E(\alpha)^\lambda$  дает  $|E(\alpha)| = 1, E(\alpha) = \pm 1$ . Другим способом можно получить это, заметив, что если  $\alpha^k$  сравнимо с целым числом по модулю  $\lambda$ , то  $1 + k(\alpha - 1)$  сравнимо с целым числом по модулю  $(\alpha - 1)^2$ ,  $k \equiv 0 \pmod{\lambda}$ ,  $(\pm e_2(\alpha))^\lambda = 1$ , и единица  $\pm e_2(\alpha)$  оказывается корнем уравнения  $X^\lambda = 1$ . 4. На основании бесконечного спуска достаточно доказать следующее: если  $p \mid o(G)$ ,  $G$  абелева и не содержит элементов порядка  $p$ , то имеется такая абелева группа  $G'$ , что  $p \mid o(G')$ ,  $G'$  абелева и не содержит элементов порядка  $p$  и  $o(G') < o(G)$ . Пусть  $a$  — элемент из  $G$ , отличный от  $e$ . Пусть  $v$  — его порядок. Тогда  $p \nmid v$ , поскольку иначе элемент  $a^{v/p}$  имел бы порядок  $p$ . Пусть  $G' = G/(a)$ . Тогда  $p \mid o(G')$ ,  $o(G') < o(G)$  и  $G'$  — абелева группа. Нужно показать, что если  $G'$  имеет элемент порядка  $p$  (например, класс смежности элемента  $b$ ), то и  $G$  имеет такой элемент. Если такое  $b$  существует, то  $b^p = a^k$ . Пусть  $n = \text{н. о. д.}(v, k)$ ,  $k = nK$ ,  $v = nN$ . Тогда  $e = a^{vK} = a^{NK} = b^{pN}$ . Значит, элемент  $b^N$  имеет порядок  $p$ , если только элемент  $b^N$  отличен от единицы. Но из равенства  $b^N = e$  вытекало бы  $p \mid N \mid v$ . [ $p \mid N$  следует из того, что  $p$  — порядок класса смежности элемента  $b$ .]

- 7.1. 1.  $x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D})$ . Если  $p$  — простое и  $p \mid (x^2 - Dy^2)$ , то  $p$  делит один из сомножителей, а потому и оба сомножителя. Обратно, если  $p \mid (x + y\sqrt{D}) \cdot (u + v\sqrt{D})$ , то  $p \mid (x^2 - Dy^2)(u^2 - Dv^2)$  и  $p \mid (x^2 - Dy^2)$  или  $p \mid (u^2 - Dv^2)$ . Поэтому  $p$  — простое число. 2. Квадратичное целое  $u + v\sqrt{D}$  при  $v = 0$  является обыкновенным целым. 5.  $-10, -7, -6, -5, -3, -2, -1, 2, 3, 5, 6, 7, 10$ . 6. Покажите, что сравнение  $u^2 \equiv -1 \pmod{p}$  при нечетном  $p$  имеет решение в том и только в том случае, когда  $p \mid (a^2 + b^2)$  при некоторых взаимно простых  $a$  и  $b$ . Таким образом, 2 разветвляется, простые  $\equiv 1 \pmod{4}$  распадаются, простые  $\equiv 3 \pmod{4}$  остаются простыми. 7. 2 разветвляется, простые  $p \equiv 1$  или  $3 \pmod{8}$  распадаются, остальные остаются простыми. 8. Простые  $\equiv \pm 1 \pmod{8}$  распадаются. 9. Если  $p \equiv 1 \pmod{3}$ , то  $f = 1, e = 2$  и  $p$  имеет 2 различных простых делителя, т. е.  $p$  распадается. Если  $p \equiv 2 \pmod{3}$ , то  $e = 1$ , т. е.  $p$  остается простым;  $(3) = (\alpha - 1)^2$ , т. е. 3 разветвляется. 10. 5 разветвляется. Если  $p \equiv 2$  или  $3 \pmod{5}$ , то  $p$  является простым как круговое целое и тем более как квадратичное целое. Если  $p \equiv 1$  или  $4 \pmod{5}$  и  $A$  — простой дивизор числа  $p$ , то  $\theta_0, \theta_1 \equiv$  целые  $\pmod{A}$ ,  $\theta_0 - \theta_1 \equiv u \pmod{A}$ ,  $u^2 \equiv (\theta_0 - \theta_1)^2 \equiv 5 \pmod{A}$ ,  $u^2 \equiv 5 \pmod{p}$  и  $p$  распадается. 11. 2 и 5 разветвляются,  $\binom{-5}{p} = \binom{-1}{p} \binom{p}{5}$

зависит только от класса  $p \pmod{4 \cdot 5}$ . В действительности это число равно  $+1$  при  $p \equiv 1, 3, 7, 9 \pmod{20}$  и  $-1$  при  $p \equiv 11, 13, 17, 19 \pmod{20}$ . 12. В каждом случае задача состоит в разложении чисел 2 и 3. Например, при  $D = -5$  число 2 разветвляется, 3 распадается и имеются 3 дивизора  $(2, *)^2 (3, \pm 1)^2$  с нормой 36. 13. Достаточно доказать, что  $\omega \equiv$  целое число  $\pmod{(p, u)}$ , но  $\omega \equiv (1 - p) \omega = [(1 - p)/2] (1 - \sqrt{D}) \equiv \frac{1}{2} (1 - p) (1 - u) =$  целое  $\pmod{(p, u)}$ .

7.2. 1. Если  $x + y \sqrt{D}$  имеет дивизор  $A$  и если дивизор  $u + v \sqrt{D}$  равен  $AB$ , то  $x + y \sqrt{D}$  делит  $u + v \sqrt{D}$  и дивизор частного равен  $B$ . 2. (a)  $(4 + 7 \sqrt{3}) = (131, u)$ , где  $4 + 7u \equiv 0 \pmod{131}$ , т. е.  $u \equiv -38$ , (b)  $(11, 3) (17, -7)$ . (c)  $(3, 1) (3, -1) (5, *)$ . (d)  $(3, *) (7, *)$ . (e)  $I$ . (f)  $(5, 2) (5, -2) (2, *)$ . 3. Немедленно следует из предложения 2.

7.3. 1.  $1 - \sqrt{2}$ ,  $(1 - \sqrt{2})^2 = 3 - 2\sqrt{2}$ ,  $(1 - \sqrt{2})^3 = 7 - 5\sqrt{2}$  имеют дивизоры  $(-1, *)$ ,  $I$ ,  $(-1, *)$  соответственно. 2. Из равенства  $u^2 - 3v^2 = -1$  следовало бы, что  $u^2 + v^2 \equiv 3 \pmod{4}$ . 3.  $2 + \sqrt{5}$  имеет норму  $-1$ .

7.4. 1. При  $A = (5, 2) (13, -5)$  тогда и только тогда  $\sqrt{-1} \equiv r \pmod{A}$ , когда  $r \equiv 2 \pmod{5}$ ,  $r \equiv -5 \pmod{13}$ , т. е.  $r \equiv -18 \pmod{65}$ . Вычисления

$$\begin{array}{ccc} -18 & -2 & \\ 65 & 5 & 1 \end{array}$$

показывают, что  $A_2$  является дивизором числа 1,  $A_1$  — дивизором  $-2 - \sqrt{-1}$ ,  $A_0$  — дивизором  $(-18 - \sqrt{-1})(-2 - \sqrt{-1})/5$ . Таким образом, имеются 4 решения  $\pm(7 + 4\sqrt{-1})$ ,  $\pm(-4 + 7\sqrt{-1})$ . 2.  $r_0 = -11/2$ ,  $a_1 = 1$ . Имеется 6 решений:  $\pm \frac{1}{2}(-11 - \sqrt{-3})$ ,  $\pm(2 + 3\sqrt{-3})$ ,  $\pm \frac{1}{2}(7 - 5\sqrt{-3})$ . 3. Решение сравнений  $r \equiv 3 \pmod{11}$ ,  $r \equiv 11 \pmod{41}$ ,  $r \equiv 20 \pmod{67}$  есть  $r \equiv 12 \pmod{30}$ ,  $r \equiv 147 \pmod{217}$ . Из таблицы

$$\begin{array}{ccc} 12 \ 147 & -2381 & 59 \ 1 \\ 30 \ 217 & 4883 & 1161 \ 3 \ 1 \end{array}$$

находим, что  $A_4, A_3, A_2, A_1, A_0$  являются дивизорами чисел 1,  $1 - \sqrt{-2}$ ,  $19 - 20\sqrt{-2}$ ,  $-39 + 41\sqrt{-2}$ ,  $-97 + 102\sqrt{-2}$  соответственно. Имеется 2 решения:  $\pm(97 - 102\sqrt{-2})$ . Другое решение:  $(11, 3)$ ,  $(41, 11)$  и  $(67, 20)$  являются дивизорами чисел  $3 - \sqrt{-2}$ ,  $3 - 4\sqrt{-2}$  и  $7 + 3\sqrt{-2}$  соответственно. Произведение этих чисел равно  $97 - 102\sqrt{-2}$ . 4.

$$\begin{array}{ccc} 8 \ 1 \ 1 & & \\ 23 \ 3 \ 2 \ 3 & & \end{array}$$

Здесь не достигается 1 и дивизор не является главным. 5.  $A_0$  делит  $(8 - \sqrt{-5})^2 = 59 - 16\sqrt{-5}$ . Так как  $(16)^{-1} \equiv -10 \pmod{23}$ ,  $(16)^{-1} \equiv -33 \pmod{23^2}$ , то  $A_0$  делит  $(-33)(59) - \sqrt{-5} \equiv 169 - \sqrt{-5} \pmod{23^2}$ . Тогда

$$\begin{array}{ccc} 169 & -7 & \\ 529 & 54 & 1 \end{array}$$

дает  $A_0$  как дивизор числа  $22 + 3\sqrt{-5}$ . 6.  $p$  делит  $N(x + y\sqrt{-1})$ , но не делит  $x + y\sqrt{-1}$ , так что  $p$  не является простым. Если  $p$  разветвляется, то  $p = 2 = 1^2 + 1^2$ . Если  $p$  распадается и  $(p, u)$  — глав-



ный дивизор, то  $p = a^2 + b^2$ . Поэтому достаточно показать, что все дивизоры — главные. В тексте было доказано, что каждый дивизор эквивалентен дивизору с нормой, не превосходящей  $2\sqrt{1/3} < 2$ , т. е. эквивалентен  $I$ . 7. Если  $p \mid x^2 + y^2$  и  $p \neq 2$ , то  $p = u^2 + v^2$  и  $p \equiv 1 \pmod{4}$ . Если  $4n = p - 1$ , то, используя рассуждение Эйлера с последовательными разностями из § 2. 4, можно показать, что  $a^{2n} - 1$  не может быть сравнимо с 0 по модулю  $p$  для всех  $a = 1, 2, \dots, p - 1$ . Следовательно,  $p \mid (a^{2n} + 1)$  при некотором  $a = 1, 2, \dots, p - 1$ . 8.  $2\sqrt{2/3} < 2$ ;  $2\sqrt{3/3} = 2$ , но при  $D = -3$  нет дивизоров с нормой 2. Последнее доказано в упр. 4. 9. Не является главным, поскольку

$$\begin{array}{cccccc} 8 & 7 & 5 & 2 & 7 & 7 & 2 & 5 & 7 & 8 \\ -1 & 3 & -6 & 7 & -9 & 2 & -9 & 7 & -6 & 3 & -1 \end{array}$$

10.

$$\begin{array}{cccccc} \frac{9}{2} & \frac{5}{2} & \frac{7}{2} & \frac{3}{2} & \frac{7}{2} & \frac{5}{2} & \frac{9}{2} \\ -1 & 7 & -3 & 5 & -5 & 3 & -7 & 1 \end{array}$$

$$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \times \\ \times \begin{pmatrix} \frac{9}{2} - \frac{1}{2}\sqrt{D} \\ 1 \end{pmatrix}$$

дает  $\frac{1}{2}(-261 + 25\sqrt{109})$ . 11. Необходимо одно приведение, прежде чем будет выполняться неравенство  $N(r - \frac{1}{2}\sqrt{D}) < 0$ .

$$\begin{array}{cccc} -\frac{41}{2} & \frac{1}{2} & \frac{9}{2} & \\ 79 & 5 & -5 & 1 \end{array} \begin{pmatrix} -4 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{9}{2} - \frac{1}{2}\sqrt{D} \\ 1 \end{pmatrix}$$

дает  $\frac{1}{2}(35 - 3\sqrt{101})$ . 12.  $r_0$  можно найти из  $(1 - \sqrt{79})^6 \equiv 266 + 344\sqrt{79} \pmod{3^6}$ ,  $(-344)^{-1} \equiv 251$ ,  $251(1 - \sqrt{79})^6 \equiv -302 - \sqrt{79}$ . Другой способ: решите сравнения  $r_0^2 \equiv 79 \pmod{3^j}$  при  $j = 1, 2, \dots, 6$ . Тогда

$$\begin{array}{cccc} -302 & 52 & -10 & \\ 729 & 125 & 21 & 1 \end{array} \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -10 - \sqrt{D} \\ 1 \end{pmatrix}$$

дает  $52 + 5\sqrt{79}$ . 13. Сразу находим  $(\frac{25}{2} - \frac{1}{2}\sqrt{-163}) = (197, 25)$ .

14.  $\pm(5 - 3\sqrt{-165})$ . 15. Дивизор элемента  $r - \sqrt{D}$  (или  $r - \frac{1}{2}\sqrt{D}$ ) имеет вид  $\prod (p, u)^\mu \cdot \prod (p, *)$ . Дивизоры, делящие этот дивизор, однозначно определяются своими нормами.

7.5. 1.

$$\begin{array}{cccc} \frac{7}{2} & \frac{5}{2} & \frac{7}{2} & \\ 1 & -3 & 3 & -1 \end{array}$$

$$\begin{pmatrix} \frac{7}{2} + \frac{1}{2}\sqrt{61} \\ \frac{5}{2} + \frac{1}{2}\sqrt{61} \end{pmatrix} \begin{pmatrix} \frac{7}{2} + \frac{1}{2}\sqrt{61} \\ \frac{5}{2} + \frac{1}{2}\sqrt{61} \end{pmatrix} / (-9) = -\frac{1}{2}(39 + 5\sqrt{61}) = \varepsilon. \text{ При нахождении } \varepsilon, \text{ применяя циклический метод}$$

к  $A_0 = (-1, *)$ , можно воспользоваться сокращениями в вычислениях из упражнений к § 7.4. Общая единица имеет вид  $\pm \varepsilon^n$ . Если  $u^2 - 61v^2 = 1$ , то  $u + v\sqrt{61} = \pm \varepsilon^{2n}$  ( $N(\varepsilon) = -1$ ). Ясно, что  $\varepsilon^2$  не имеет целых коэффициентов;  $\varepsilon^3 = -29\,718 - 3805\sqrt{61}$ ;  $\varepsilon^4$  не имеет целых коэффициентов. Таким образом, наименьшее решение уравнения Пелля равно  $u + v\sqrt{61} = \pm \varepsilon^6$ , т. е.  $v = 2 \cdot 29\,718 \cdot 3805$ .  
 2. Применяя циклический метод к  $A_0 = (-1, *)$ , получаем  $\varepsilon = \frac{1}{2}(-261 + 25\sqrt{109})$ . Наименьшее решение уравнения Пелля равно  $\varepsilon^6$ .

7.6. 1. 2 остается простым,  $(-1, *) \sim I \sim (3, \pm 1)$ ,  $\sqrt{D/3} < 5$ . Все дивизоры — главные;  $I$  — система представителей. 2. 2, 3, 7 остаются простыми,  $\sqrt{|D|/3} < 9$ ; 5 разветвляется и  $(5, *)$ ,  $(5, *)^2 \sim I$  образуют систему представителей. 3. Применяя циклический метод к  $(2, 0)$ , получим  $(2, 0) \sim (-1, *)$ ,  $(2, 1)^3 \sim (3, -1) \sim (-1, *)$ ,  $(2, 0) \sim (2, 1)^3 \sim (-1, *)$ ,  $(3, -1)$ ; отсюда  $(-1, *) \sim I$ ,  $(2, 0)^4 \sim I$ . Пусть  $A = (2, 0)$ . Согласно циклическому методу,  $A^2 \not\sim I$ ;  $\sqrt{D/3} < 7$ ;  $(3, -1) \sim A$ ;  $(5, *) \sim (-1, *)$ ,  $(2, 1)(3, 1) \sim A^3 A^3 \sim A^2$ . Таким образом,  $A, A^2, A^3, A^4 \sim I$  — система представителей. 4. Согласно циклическому методу,  $(-1, *) \sim (2, 1)^2 \sim (-1, *)$ ,  $(5, *) \not\sim I$ . Следовательно,  $(5, *) \sim I$ ,  $(2, 1)^4 \sim I$ . Циклический метод, примененный к  $(2, 1)$ , дает длинный цикл дивизоров (8 дивизоров) и показывает, что  $(2, 1) \sim (7, 2) \not\sim I$ . Так как  $\sqrt{D/3} < 11$ , то 4 степени  $(2, 1)$  образуют систему представителей. 5. Согласно циклическому методу,  $(2, *) \sim (5, -1)(13, -1) \not\sim I$ ,  $(3, *) \sim (43, *)$ . Тогда  $(5, -1) \sim (5, -1) \times (13, -1)(13, 1) \sim (2, *)$ ,  $(13, 1)$ . Для нахождения  $(5, -1)^2$  положим  $r = -1 + 5k$ ,  $-129 \equiv (-1 + 5k)^2 \pmod{25}$ ,  $k \equiv 13 \equiv -2 \pmod{5}$ ,  $r \equiv -11$ . Это дает  $(5, -1)^2 \sim (2, *) \cdot (5, 1) \not\sim I$ ;  $(5, -1)^3 \sim (2, *)$ . При  $A = (5, -1)$  отсюда следует, что  $A^2 \sim (2, *)$ ,  $A^3 \sim (2, *)$ ,  $A^4 \sim (2, *)$ ,  $A^5 \sim (5, 1)$ ,  $A^6 \sim I$ . Это не затрагивает дивизор  $(3, *)$ . Пусть  $B = (3, *)$ . Тогда  $B^2 \sim I$ ,  $AB \sim (11, -5)$  (короткое вычисление),  $A^2B \sim (7, 2)$  (снова короткое вычисление),  $A^3B \sim (2, *)$ ,  $A^4B \sim (7, -2)$ ,  $A^5B \sim (11, 5)$ . Так как  $2\sqrt{D/3} < 14$ , при этом получают все возможные неглавные дивизоры, за исключением простых дивизоров числа 13. Однако из  $(2, *) \sim (5, -1)(13, -1)$  следует, что  $A^3 \sim A(13, -1)$ ,  $(13, -1) \sim A^2$ ,  $(13, 1) \sim A^4$ . Таким образом,  $A^i B^j$ ,  $i = 0, 1, 2, 3, 4, 5$ ,  $j = 0, 1$  — система представителей. 6. Пусть  $A = (2, *)$ ,  $B = (3, *)$ ,  $C = (5, *)$ . Тогда  $I, A, B, C, AB, AC, BC, ABC$  — множество представителей. 7.  $(2, *)$ ,  $(3, *)$ ,  $(5, *)$  делит  $15 - \sqrt{D}$ . 8.  $r^2 + 163s^2$  — простое число, поэтому  $r \neq 0$  и  $s \neq 0$ . Если  $u = 0$ , то  $\sqrt{-163}$  делит  $(2x + 1)$ , что невозможно. Если  $v = 0$ , то  $u$  — целое, делящее  $\frac{1}{2}(k + \sqrt{D})$ , так что  $u = \pm 1$ .

7.7. 1. См. упр. 15 к § 7.4. 2. Предположим, что  $A \sim B$  и что применение циклического метода к  $A$  или  $B$  увеличивает их нормы. Пусть дивизор  $x + y\sqrt{D}$  равен  $A\bar{B}$ . Пусть  $a = N(A)$ ,  $b = N(B)$ . Так как  $a \leq \sqrt{|D|/3}$ ,  $b \leq \sqrt{|D|/3}$ , то  $x^2 - Dy^2 \leq |D|/3$ ; отсюда  $y = 0$  или  $\pm 1/2$ . Если  $y = 0$ , то  $x$  — целое число и рассуждение из текста показывает, что  $A = B$ . Если  $y = \pm 1/2$ , то, как и в тексте, через  $r$  обозначим наименьшее полуцелое  $r \equiv \frac{1}{2}\sqrt{D} \pmod{A}$ , а через  $r'$  — наименьшее полуцелое, для которого  $r' \equiv \frac{1}{2}\sqrt{D} \pmod{B}$ . Тогда  $|r| = |r'|$  и  $a = b$ . Если  $|r| = a/2$ , то, как и в тексте,  $D = -3$ ; в этом случае из неравенства  $a \leq \sqrt{|D|/3} = 1$  вытекает, что  $A = I = B$ .

В противном случае  $B$  следует за  $A$ . 4. Теорема. Данная матрица представима в виде (4) тогда и только тогда, когда  $X \geq Z \geq W \geq 0$ ,  $X \geq Y \geq W \geq 0$  и  $XW - YZ = \pm 1$ . Такое представление единственно. Доказательство необходимости этих 3 условий несложно. Предположим, что алгоритм Евклида, примененный к  $X, Z$ , дает:  $X = q_0Z + r_1$ ,  $Z = q_1r_1 + r_2$ ,  $r_1 = q_2r_2 + r_3$ ,  $\dots$ ,  $r_{m-1} = q_mr_m + 1$  ( $X$  и  $Z$  взаимно просты согласно  $XW - YZ = \pm 1$ ). Тогда матрица в правой части (4) имеет первым столбцом  $X, Z$ , если  $n_k = q_0$ ,  $n_{k-1} = q_1$ ,  $\dots$ ,  $n_2 = q_m$ ,  $n_1 = r_m$  (и, в частности,  $k = m + 2$ ). Определители обеих частей равны тогда и только тогда, когда  $XW - YZ = (-1)^k$ . Если это равенство не выполняется, то к алгоритму Евклида добавим еще  $r_m = (r_m - 1) \cdot 1 + 1$ , так что  $n_k = n_{m+3} = q_0$ ,  $n_{k-1} = q_1$ ,  $\dots$ ,  $n_3 = q_m$ ,  $n_2 = r_m - 1$ ,  $n_1 = 1$ . Тогда обе части (4) имеют равные определители и равные первые столбцы. Таким образом,  $X(W - W') = Z(Y - Y')$ , и надо доказать, что  $W = W'$ ,  $Y = Y'$ . Если  $Y$  и  $Y'$  отличны от нуля, то сравнение  $Y \equiv Y' \pmod{X}$  и неравенства  $X \geq Y \geq 0$ ,  $X \geq Y' \geq 0$  позволяют сделать нужный вывод. Так как  $Y \geq W$ ,  $Y' \geq W'$ , то  $Y$  и  $Y'$  отличны от нуля. 5. Есть два способа расстановки знаков в правой части (4), для того чтобы получить такое же произведение, как и в правой части (2), а именно:  $n_1$  можно приписать любой знак. Любой расстановке знаков соответствует расстановка знаков при  $X, Y, Z, W$ ; абсолютная величина этих чисел остается неизменной. Если даны  $|X|$  и  $|Z|$ , то для (4) имеются две возможности: одна — с нечетным, а другая — с четным числом множителей  $j$ ;  $X$  и  $Y$  имеют одинаковые знаки тогда и только тогда, когда  $n_1 > 0$ ;  $X$  и  $W$  имеют одинаковые знаки в том и только в том случае, когда  $j$  нечетно. Оставшийся знак перед (2) позволяет осуществить каждую из 8 возможных расстановок знаков единственным способом. 6. В доказательстве из текста  $x^2 \geq r^2y^2$ , поскольку  $x = bu$ ,  $y = bv$ ,  $u^2 - Dv^2 = 1$ ,  $D > r^2$ . Аналогично,  $ab + Dy^2 > (s - |b|)^2 y^2$ .

7.8. 1. Рассуждения из текста показывают, что  $p \mid (x^2 - Dy^2)$  при некоторых взаимно простых  $x, y$  тогда и только тогда, когда  $p$  распадается в квадратичных целых детерминанта  $D$  (при  $p \neq 2$ ). Если  $D$  — квадрат, то всегда можно найти такие взаимно простые  $x, y$ , что  $p \mid (x^2 - Dy^2)$ . Пусть  $p_0 \mid (x_0^2 - Dt^2y_0^2)$  при взаимно простых  $x_0, y_0$ ; предположим, что  $p_0 \equiv p_1 \pmod{4Dt^2}$ ; надо показать, что  $p_1 \mid (x_1^2 - Dt^2y_1^2)$  при взаимно простых  $x_1, y_1$ . Здесь  $x_0$  и  $ty_0$  могут не быть взаимно простыми, только если  $p_0$  делит  $t$ ; в этом случае  $p_1 = p_0$ . Если  $p_0 \neq p_1$ , то, согласно предположению, существуют такие взаимно простые  $x_2, y_2$ , что  $p_1 \mid (x_2^2 - Dy_2^2)$ . Положим  $d = \text{н. о. д.}(t, y_2)$ ,  $t' = t/d$ ,  $y'_2 = y_2/d$ ,  $x_1 = t'x_2$ ,  $y_1 = y'_2$ . 3. Если  $q = 2$ , то среди четырех классов 1, 3, 5, 7 только 1 является квадратом. Пусть  $q \neq 2$ . Если  $y$  взаимно просто с  $q$  и  $x^2 \equiv y^2 \pmod{4q}$ , то  $(xy^{-1})^2 \equiv 1 \pmod{4q}$ , т. е.  $x = ty$ , где  $t^2 \equiv 1 \pmod{4q}$ . Тогда  $t \equiv \pm 1 \pmod{4}$  и  $t \equiv \pm 1 \pmod{q}$ , и, согласно китайской теореме об остатках, для  $t$  имеется в точности 4 возможности (а именно,  $t = \pm 1$ ,  $t = 2q \pm 1$ ). Таким образом, при возведении в квадрат 4 элемента переходят в один. 4. Если  $D = -1$ , то 1 распадается, так что не распадается  $-1$ . Если  $D = 2$ , то 1 распадается, так что распадается и  $-1$ , а остальные классы не распадаются. Когда  $D = -2$ ,  $3 \mid 1^2 + 2 \cdot 1^2$  распадается, а  $-1$ ,  $-3$  не распадаются. 5. Пусть  $a = \text{Pr}^\mu$  взаимно просто с  $4D$ . Если  $p$  распадается, то  $p^\mu$  принадлежит распадающемуся классу. Если  $p$  остается простым, то  $A = (p)^\nu A'$ , где  $A$  взаимно просто с  $p$ ,  $\mu = 2\nu$  и  $p^\mu = (p^\nu)^2$  принадлежит распадающемуся классу. Следовательно,  $a$  принадлежит распадающемуся классу. 6. Пусть  $S$  — представители распадающихся, а  $N$  — нераспадающихся классов. Поскольку умножение на элементы из  $S$

переводит  $S$  в  $S$ , оно должно переводить  $N$  в  $N$ . Таким образом, при умножении  $S$  на  $N$  всегда получается  $N$ . Поскольку умножение на  $N$  переводит  $S$  в  $N$ , то оно должно переводить  $N$  в  $S$ , что и требовалось доказать. 7.  $\left(\frac{-7}{15}\right) = +1$  означает, что если  $p$  — простое число, сравнимое с 15 по модулю 4·7, то  $-7$  является квадратом по модулю  $p$ . (Например,  $6^2 \equiv -7 \pmod{43}$ .) 8. Достаточно рассмотреть случай простого  $q$ . Пусть  $p = p_1 \cdot \dots \cdot p_\mu p'_1 \cdot \dots \cdot p'_\nu$ , где  $p_i \equiv 1 \pmod{4}$  и  $p'_i \equiv 3 \pmod{4}$ . Тогда, как и требуется,

$$\left(\frac{q}{p}\right) = \prod \left(\frac{q}{p_i}\right) \prod \left(\frac{q}{p'_i}\right) = \prod \left(\frac{p_i}{q}\right) \prod \left(\frac{-p'_i}{q}\right) = \left(\frac{(-1)^{\nu_p}}{q}\right).$$

9. Предположим, что теоремы Эйлера справедливы для детерминанта  $D'$ . Каждый класс целых по модулю  $4D$ , взаимно простой с  $4D$ , содержится в некотором классе по модулю  $4D'$ , взаимно простом с  $4D'$ . Назовем класс распадающимся классом для  $D$ , если он содержится в распадающемся классе для  $D'$ . Рассуждения из упр. 1 показывают, что если  $p$  принадлежит распадающемуся классу для  $D$ , то  $p \mid (x^2 - Dy^2)$  при взаимно простых  $x, y$ . Отсюда легко выводятся теоремы Эйлера.

- 7.9. 1. Согласно упр. 5 к § 7.8, если  $m = N(A)$ , где  $A$  взаимно просто с  $4D$ , то  $\left(\frac{D}{m}\right) = +1$ . Так как  $\left(\frac{D}{m}\right) = \left(\frac{k}{m}\right) \left(\frac{m}{p_1}\right) \dots \left(\frac{m}{p'_\nu}\right)$ , где  $k = D/p_1 \cdot \dots \cdot p_\mu (-p'_1) \cdot \dots \cdot (-p'_\nu) \equiv D \pmod{4}$  (и в действительности  $k \equiv D \pmod{8}$ , если  $2 \mid D$ ), то символ Якоби равен просто произведению знаков в роде дивизора  $A$ . Согласно § 8.3, каждый дивизор эквивалентен такому дивизору  $A$ . Если задан любой возможный характер, то используйте китайскую теорему об остатках для нахождения такого целого  $m$ , что  $\left(\frac{k}{m}\right), \left(\frac{m}{p_1}\right), \dots, \left(\frac{m}{p'_\nu}\right)$  являются соответствующими знаками. По теореме Дирихле, существует простое  $p \equiv m \pmod{4D}$ . Так как  $\left(\frac{D}{p}\right) = 1$ , то  $p$  распадается и его простые делители имеют выделенный характер. 2. Только (3) нетривиально. Так как  $(x/y)^2 \equiv -n \equiv (u/v)^2 \pmod{k}$ , то  $xv \equiv \pm yu \pmod{k}$ . При необходимости измените знак  $y$ , для того чтобы получить  $xv \equiv yu$ . Тогда  $k^2 = (xu + yuv)^2 + n(xv - yu)^2$  делится на  $k^2$  и дает  $1 = a^2 + nb^2$ . Если  $b = 0$ , то  $xv = yu$ ,  $x^2k = x^2u^2 + nx^2v^2 = u^2k$ ,  $x = \pm u$ ,  $v = \pm y$ , что и требуется. Если  $b \neq 0$ , то  $n = 1$ ,  $a = 0$ ,  $xu = -yv$  и  $x^2k = v^2k$ ,  $x = \pm v$ ,  $y = \pm u$ . При  $n \not\equiv 1 \pmod{4}$  получается более легкое доказательство, если использовать теорию дивизоров. 3. Если  $D = -165$ , то  $A \sim \bar{A}$  для всех дивизоров  $A$ ;  $A_1 \neq \bar{A}_1$ , поскольку (1) и (2) показывают, что  $(2, *)$ ,  $(3, *)$ ,  $(5, *)$ ,  $(11, *)$  не делят  $A_1$ . Если дивизор элемента  $u + v\sqrt{D}$  равен  $\bar{A}_1 A_2$ , а дивизор  $x + y\sqrt{D}$  равен  $A_1 A_2$ , то  $x \pm y\sqrt{D}$  не равно единице, умноженной на  $u + v\sqrt{D}$ , что противоречит (3). Если  $x + y\sqrt{D}$  имеет дивизор  $(p, u)^n$ , то  $(p)(p, u)^{n-2}$  является главным дивизором, скажем дивизором элемента  $r + s\sqrt{D}$ , и снова (3) не выполняется. 4. Если  $a$  четно, то  $b$  нечетно. Предположим, что  $a$  нечетно. Число  $ak$  является нормой дивизора числа  $ax + y\sqrt{D}$ , где  $D = -ab$ . Этот дивизор имеет вид  $(p_1, *) (p_2, *) \dots (p_n, *) A$ , где  $k = N(A)$ . Если  $k$  — простое число, то (1) и (2) очевидны. Относительно (3): если  $k = au^2 + bv^2$ , то  $au + v\sqrt{D}$  имеет дивизор  $(p_1, *) \dots (p_n, *) B$ , где  $k = N(B)$ . Если  $k$  — простое, то  $B = A$  или  $B = \bar{A}$ , и  $au \pm v\sqrt{D} = \pm 1 \cdot (ax + y\sqrt{D})$ , что и требуется. Обратно, рассуждения из упр. 3 показывают, что если  $A$  — не простой дивизор,

то существует  $c + d \sqrt{D}$  с нормой  $ak$ , не равное  $\pm(ax \pm y \sqrt{D})$ ; так как  $a$  должно делить  $c$ , то это противоречит (3). 5. Исключениями являются  $165 + 2^2 = 0.165 + 13^2$ ,  $165 + 14^2 = 361 = 0.165 + 19^2$ ,  $165 + 26^2 = 0.165 + 29^2$ ,  $165 + 28^2 = 2^2.165 + 17^2$  и  $165 + 32^2 = 2^2 \cdot 165 + 23^2$ . 6.  $5 \not\equiv 3 \pmod{4}$ . Существуют два класса с различными характерами («++» и «--»). 7. Если  $p \equiv 3 \pmod{4}$ ,  $p \equiv 3$  или  $7 \pmod{10}$ , то  $\binom{-5}{p} = \binom{-1}{p} \cdot \binom{p}{5} = (-1)(-1) = +1$ , и  $p$  распадается при  $D = -5$ . Характер его простых дивизоров есть «--». Произведение простого дивизора числа  $p_1$  на простой дивизор числа  $p_2$  принадлежит главному роду, а потому и главному классу. 8.  $-Dy^2 \equiv -D$  или  $0 \pmod{4D}$ ;  $p + D = 180 = 5 \cdot 6^2$ . Подбором находим:  $5 \equiv 20^2 \pmod{79}$ . Тогда легко найти, что  $59^2 \equiv 5 \pmod{4 \cdot 79}$  и  $38^2 \equiv 180 \pmod{4 \cdot 79}$ . Отсюда получается, что  $733 = 38^2 - 79 \cdot 3^2$ . Разделите на 3, 5, ..., 23, для того чтобы доказать простоту числа 733. Таким образом, 733 распадается и его простые дивизоры являются главными. Сравнение  $101 \equiv 733 \pmod{4D}$  не только показывает, что 101 распадается, но и что его простые дивизоры принадлежат тому же роду, что и простые дивизоры числа 733, а именно главному роду. Надо доказать, что они не принадлежат главному классу. Подбором находим:  $79 \equiv 1089 = 33^2 \pmod{101}$ . Циклический метод дает  $(101, 33) \sim (2, *) (5, 2)$ , и, используя  $B = (3, 1)$ , как и в § 7.6, получим  $(2, *) (5, 2) \sim I \cdot B^2 \not\sim I$ .

7.10. 1.  $I$  и  $(2, *) (3, *) (5, *)$  — главные дивизоры; 4 двусторонних класса. 2.  $I$  и  $(31, *)$  — главные дивизоры; 1 двусторонний класс. 3.  $I$ ,  $(2, *)$ ,  $(31, *)$ ,  $(2, *) (31, *)$  — главные дивизоры; дивизор  $(-1, *)$  не является главным; 2 двусторонних класса. 4.  $I$ ,  $(-1, *) (2, *) (7, *)$ ,  $(3, *) (5, *)$  и  $(-1, *) (2, *) (3, *) (5, *) (7, *)$  — главные дивизоры. Характеры  $-+-+$ ,  $--++$ ,  $----$ ,  $+---$  дивизоров  $(-1, *)$ ,  $(2, *)$ ,  $(3, *)$ ,  $(7, *)$  показывают, что все 8 характеров с четным числом минусов встречаются как характеры двусторонних классов. Следовательно, имеется по меньшей мере 8 двусторонних классов. Поэтому есть в точности 8 двусторонних классов. 5.  $I$ ,  $(-1, *)$ ,  $(61, *)$  и  $(-1, *) (61, *)$  — главные дивизоры; 1 двусторонний класс. 6.  $(-1, *)$  не принадлежит главному роду;  $I$ ,  $(-1, *) (2, *)$ ,  $(-1, *) \times (59, *)$  и  $(2, *) (59, *)$  — главные дивизоры; 2 двусторонних класса. 7. При  $D > 0$  имеется по меньшей мере 4 главных двусторонних дивизора. Если  $D$  — простое и  $D \equiv 1 \pmod{4}$ , то имеется в точности 4 двусторонних дивизора. Таким образом,  $(-1, *)$  — главный дивизор. Если  $D$  — простое и  $D \equiv 3 \pmod{4}$ , то  $(-1, *)$  не принадлежит главному роду. 8. Имеется 8 дивизоров  $(-1, *)^a (p, *)^b (q, *)^c$ . Характер дивизора  $(-1, *)$  равен  $--$ . Таким образом, существуют 2 класса, каждый из которых образует отдельный род. Характер класса  $(p, *) (q, *) \sim (-1, *)$  равен  $--$ , поэтому  $(p, *)$  и  $(q, *)$  не могут одновременно иметь характер  $--$  или  $++$ . 9. Цикл  $I$  содержит  $(-1, *)$ , скажем  $(-1, *) = A_{2j+1}$ . Тогда  $N(A_i) = -N(A_{2j+1-i})$ , следовательно,  $N(A_j) = -N(A_{j+1})$ . При  $D = 13$  [имеем  $j = 0$  и  $N\left(\frac{3}{2} - \frac{1}{2} \sqrt{13}\right) = -1$ , что, как и требуется, дает  $3^2 - 13 = -2^2$ ,  $13 = 3^2 + 2^2$ . При  $D = 233$  имеем  $a_4 = -a_5 = 4$ ,  $r_4 = 13/2$ ; отсюда следует, что  $13^2 + (2 \cdot 4)^2 = D$ .

7.11. 1.  $n = 1 \geq s$  дает  $s = 1$ ,  $h = sa = a$ , т. е. каждый класс является двусторонним. 2. В VI дивизор  $(-1, *)$  имеет характер  $--$ . Вторым знаком характера дивизора  $(p, *) \sim (-1, *) (2, *)$  равен  $+1$ , поскольку  $p \equiv 3 \pmod{8}$ ,  $D \equiv -2 \pmod{8}$ . Следовательно, первый знак также должен быть равен  $+1$ . 3. Если  $g = a$ , то  $n = s$ .

8.1. 1. (a) Методы из гл. 7 показывают, что единственными квадратичными целыми с дивизором  $(3, 1)$  являются  $\pm \frac{1}{2}(1 - \sqrt{-11})$ ; они не принадлежат подпорядку. (b)  $(2)$  является дивизором числа 2, а  $(2)(3, 1)$  — дивизором  $\pm(1 - \sqrt{-11})$ . (c)  $(3, 1)^2$  является дивизором  $\pm(1 - \sqrt{-11})^2/4 = \pm \frac{1}{2}(5 + \sqrt{-11})$ , а  $(3, 1)^3$  — дивизор  $\pm(4 - \sqrt{-11})$ . (d)  $(5, 2)(3, -1)$  — дивизор  $2 - \sqrt{-11}$ . (k) Если  $x, y$  — нечетные целые, то  $y \pm x$  делится на 4 при одном из выборов знака и  $(x \pm y\sqrt{-11})(1 \pm \sqrt{-11})/4$  имеет целые коэффициенты. 2. В пункте (b) упр. 1 положим  $A = I, B = (3, 1), C = (2)$ . Если  $CD \sim I$ , то  $AC \sim BC$  влечет за собой  $A \sim B$ . 3.  $(13, 5)$  делит  $5 - \sqrt{-1}$ . Следовательно,  $(13, 5)$  делит  $30 - 6\sqrt{-1}$  и  $4 - \sqrt{-36}$  — квадратичное целое с дивизором  $(2, *)^2(13, 5)$ . Следующий шаг приводит  $-4$  по модулю 4 и дает  $-\sqrt{-36}$  с дивизором  $(2, *)^2(3, 1)(3, -1)$ . Таким образом, получаются дивизоры  $(13, 5), (2, *)^2, (3, 1)(3, -1), (2, *)^2, (3, 1)(3, -1), \dots$ . Дивизоры  $(2, *)^2$  и  $(3, 1)(3, -1)$  являются главными, поэтому ни один из них не эквивалентен  $(13, 5)$ . 5. При  $D' \equiv 1 \pmod{4}$  через  $v$  обозначим такое наименьшее положительное целое, что  $u + v\omega$  принадлежит данному порядку. (Порядок содержит по крайней мере один элемент  $\pm(x + y\omega)$  с  $y \neq 0$ .) Если  $x + y\omega$  — произвольный элемент порядка, положим  $y = qv + r$ , где  $0 \leq r < v$ . Так как  $x + y\omega = q(u + v\omega) + r\omega = (x - qu) + r\omega$  принадлежит данному порядку, то  $r = 0$ . Таким образом, данный порядок является порядком индекса  $v$ . Тот же метод можно применить и при  $D' \not\equiv 1 \pmod{4}$ . 6. Пусть  $A$  — данный дивизор, взаимно простой с 3. При  $D = 2$  все дивизоры являются главными, так что  $A$  равен дивизору  $x + y\sqrt{2}$  при некоторых  $x, y$ . Общий элемент с дивизором  $A$  имеет вид  $\pm(x + y\sqrt{2}) \cdot (1 - \sqrt{2})^{2n}$ . По модулю 3 он равен  $\pm(x + y\sqrt{2})$  или  $\pm(-y + x\sqrt{2})$  и принадлежит данному порядку при некотором  $n$  тогда и только тогда, когда  $x$  или  $y$  делится на 3. Таким образом, дивизор  $(-1, *)$  не является главным. Если  $A$  — не главный дивизор, то главным является дивизор  $A(-1, *)$ . 7.  $(1 - \sqrt{D})^3 = 1 + 3D - (3 + D)\sqrt{D} \equiv 0 \pmod{8}$ . Если  $D$  отрицательно и  $\neq -1$  или  $-3$ , то единственными единицами являются  $\pm 1$ . Следовательно, при  $D \neq -3$  ни один элемент порядка не имеет такой же дивизор, что и  $\frac{1}{2}(1 - \sqrt{D})$ . При  $D = -3$  имеется только один класс дивизоров. 10.  $11 + 1^2$  не представимо ни в одном из данных 4 видов, поэтому число 11 не должно быть удобным. Это показано в упр. 7. Далее,  $13 + 1 = 2 \cdot 7, 13 + 4 = 17, 13 + 9 = 2 \cdot 11, 13 + 16 = 29, 13 + 25 = 2 \cdot 19, 13 + 36 = 7^2$ , так что число 13 должно быть удобным. При  $D = -13$   $I$  и  $(2, *)$  образуют множество представителей. Среди чисел от 80 до 89 только 85 и 88 удовлетворяют критерию Эйлера.

8.2. 2. Сравнение  $a^2 \equiv -1 \pmod{65}$ , или, что то же самое,  $a^2 \equiv -1 \pmod{5}$  и  $a^2 \equiv -1 \pmod{13}$ , имеет решения  $a \equiv \pm 2 \pmod{5}, a \equiv \pm 5 \pmod{13}$ , т. е.  $a \equiv \pm 8$  или  $\pm 18 \pmod{65}$ . Циклический метод дает

$$\begin{array}{cccc} -18 & -2 & 0 & \\ 65 & 5 & 1 & 1 \end{array}$$

Обратив эту таблицу и положив  $u = 0, v = 1$ , найдем

$$\begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 7 \end{pmatrix},$$



$4^2 + 7^2 = 65$ . Таким же образом решение  $-8$  дает  $1^2 + 8^2 = 65$ . 3.  $a^2 \equiv -19 \pmod{121}$  дает  $a^2 \equiv 3 \pmod{11}$ ,  $a \equiv \pm 5 \pmod{11}$ ,  $a \equiv \pm 5 + 11k \pmod{121}$ ,  $a \equiv \pm 49 \pmod{121}$ . Циклический метод показывает, что форма  $121r^2 + 98rs + 20s^2$  эквивалентна  $5g^2 - 2gh + 4h^2$ . Последняя форма эквивалентна данной форме. Обращая шаги вычислений и перемножая матрицы так же, как и в основном тексте, получим в качестве представления  $g = -5$ ,  $h = -2$ ; следовательно,  $x = 2$ ,  $y = -5$  является решением исходной задачи. 4.  $x = 8$  является решением сравнения  $x^2 \equiv -5 \pmod{23}$ . Тогда

$$\begin{array}{ccccc} 20 & 7 & 1 & 8 & \\ 15 & 27 & 2 & 3 & 23 \end{array}$$

дает решение  $x = -11$ ,  $y = 8$ . 5. Решение  $a = 49$  сравнения  $a^2 \equiv 79 \pmod{3 \cdot 43}$  не приводит к представлению. Решение  $a = -49$  приводит к

$$\begin{array}{ccccc} 59 & 22 & 8 & -5 & -49 \\ 42 & 81 & 5 & -3 & 18 & 129 \end{array}$$

и к представлению  $x = -15$ ,  $y = 13$ . 6. Два решения 19 и 33 сравнения  $a^2 \equiv -3 \pmod{182}$  дают два представления  $x = -1$ ,  $y = 10$  и  $x = -6$ ,  $y = 11$ .

8.3. 1.  $I$  и  $(-1, *)$  образуют систему представителей (§ 7.6). Следовательно, формы  $x^2 - 67y^2$  и  $-x^2 + 67y^2$  обладают требуемым свойством. 2.  $x^2 + 165y^2$ ,  $2x^2 + 2xy + 83y^2$ ,  $3x^2 + 55y^2$ ,  $5x^2 + 33y^2$ ,  $6x^2 + 6xy + 174y^2$ ,  $10x^2 + 10xy + 19y^2$ ,  $11x^2 + 15y^2$ ,  $13x^2 + 4xy + 13y^2$  и эти же формы, умноженные на  $-1$ . 3.  $x^2 - 79y^2$ ,  $3x^2 \pm 2xy - 26y^2$ ,  $5x^2 \pm 4xy - 15y^2$ ,  $-x^2 + 79y^2$ . 4.  $x^2 + 161y^2$ ,  $3x^2 \pm 2xy + 54y^2$ ,  $9x^2 \pm 2xy + 18y^2$ ,  $6x^2 \pm 2xy + 27y^2$ ,  $2x^2 + 2xy + 81y^2$ ,  $7x^2 + 23y^2$ ,  $10x^2 \pm 6xy + 17y^2$ ,  $11x^2 \pm 4xy + 15y^2$ ,  $5x^2 \pm 4xy + 33y^2$ ,  $14x^2 + 14xy + 15y^2$  и эти же формы, умноженные на  $-1$ . 5.  $x^2 + 11y^2$ ,  $3x^2 \pm 2xy + 4y^2$  и эти же формы, умноженные на  $-1$ . 6.  $\pm(x^2 - 18y^2)$ .

8.4. 1. Число приведенных бинарных квадратичных форм с данным детерминантом, очевидно, конечно. 2. Пусть задана единица с нормой 1; пусть  $M$  есть  $2 \times 2$ -матрица, соответствующая умножению  $ax + (b - \sqrt{D})y$  на эту единицу. Доказательство из текста показывает, что  $E_1^n M$  получается вырезанием из  $E_1^N$  для большого  $N$ ; отсюда следует, что  $M = \pm E_1^k$  при целом  $k$ . Таким образом, данная единица равна  $\pm \varepsilon^k$ . Если  $ax^2 + 2bxy + cy^2$  — приведенная форма, то циклический метод дает  $A = Q A Q^t$ , где

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \quad Q = \begin{pmatrix} n_1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} n_2 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_k & -1 \\ 1 & 0 \end{pmatrix},$$

причем числа  $n$  равны частным  $(r_i + r_{i+1})/a_{i+1}$ . Тогда единицу  $\varepsilon = g + h\sqrt{D}$  можно найти, используя формулу

$$Q = \begin{pmatrix} g + bh & -ah \\ ch & g - bh \end{pmatrix}$$

( $Q$ ,  $a$ ,  $b$ ,  $c$  известны), которая следует из формул в тексте. Применить циклический метод к  $-ax^2 + 2bxy - cy^2$  — то же самое, что применить его к  $ax^2 + 2bxy + cy^2$  и изменить знаки в нижней строке. Таким образом, одна из этих форм приведена тогда и только тогда, когда приведена вторая, и если обе эти формы приведены и эквивалентны,

то циклический метод задает эквивалентность в явном виде

$$\begin{pmatrix} -a & b \\ b & -c \end{pmatrix} = Q \begin{pmatrix} a & b \\ b & c \end{pmatrix} Q^t, \quad Q = \begin{pmatrix} n_1 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_j & -1 \\ 1 & 0 \end{pmatrix}.$$

Это соответствует умножению на  $u + v\sqrt{D}$  с последующим делением на  $a$ , где  $N(u + v\sqrt{D}) = -a^2$ . Тогда  $(u + v\sqrt{D})/a$  — квадратичное целое с нормой  $-1$ . В явном виде оно равно  $g + h\sqrt{D}$ , где

$$Q = \begin{pmatrix} g + bh & -ah \\ -ch & -g + bh \end{pmatrix}.$$

Обратно, если  $g + h\sqrt{D}$  — произвольное квадратичное целое с нормой  $-1$ , то эта формула дает собственную эквивалентность форм  $ax^2 + 2bxy + cy^2$  и  $-ax^2 + 2bxy - cy^2$ . Доказательство того, что приведенная выше процедура нахождения единицы с нормой  $-1$  (если такая единица существует) дает единицу, квадрат которой равен  $\varepsilon$ , кажется довольно хитрым. По-видимому, простейший метод состоит в том, чтобы заметить, что с точностью до знаков

$$Q = \begin{pmatrix} |n_1| & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} |n_2| & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} |n_k| & 1 \\ 1 & 0 \end{pmatrix}.$$

3. Циклический метод, примененный к  $x^2 - 67y^2$ , и формулы из § 8.2 показывают, что  $QAQ^t = A$ , где

$$A = \begin{pmatrix} 1 & 8 \\ 8 & -3 \end{pmatrix}, \quad Q = \begin{pmatrix} -5 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 16 & -1 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} -96\,578 & 5967 \\ 17\,901 & -1106 \end{pmatrix}.$$

$$-ah = 5967, \quad h = -5967, \quad g + bh = -96\,578, \quad g = -48\,842.$$

4. Циклический метод дает

$$\begin{pmatrix} 1 & \frac{7}{2} \\ \frac{7}{2} & -3 \end{pmatrix} = \begin{pmatrix} 37 & 5 \\ -15 & -2 \end{pmatrix} \begin{pmatrix} -1 & \frac{7}{2} \\ \frac{7}{2} & 3 \end{pmatrix} \begin{pmatrix} 37 & -15 \\ 5 & -2 \end{pmatrix}.$$

Тогда  $-ah = 5$ ,  $h = 5$ ,  $g + bh = 37$ ,  $g = 39/2$  и единица равна  $\frac{1}{2}(39 + 5\sqrt{61})$ . 5. Так как  $(5, 1)$  делит  $1 - \sqrt{11}$ , то  $(5, 1)$  делит  $3 - \sqrt{99}$  и циклический метод дает

$$\begin{array}{ccccccccc} 3 & & -3 & & 8 & & 6 & & 3 & & 7 & & 8 \\ 5 & & -20 & & 5 & & -7 & & 9 & & -10 & & 5 \end{array}$$

Дивизоры  $(5, 1)$  и  $(-1, *)$   $(2, *)$   $(5, -1)$  эквивалентны, поскольку они соответствуют формам, принадлежащим одному периоду;  $(5, 1)^2 \sim (-1, *)$   $(2, *)$ ,  $(5, 1)^4 \sim I$ , и ни одна из степеней дивизора  $(5, 1)$  не эквивалентна дивизору  $(-1, *)$ . Каждая форма эквивалентна форме, для которой  $0 < b < \sqrt{99}$ ,  $b + |a| > \sqrt{99}$  и  $b + |c| > \sqrt{99}$ . Легко проверить, что все такие формы эквивалентны формам, принадлежащим найденным 8 периодам  $(-1, *)^a (5, 1)^b$ . 6.  $(5, 2)^3 \sim (11, *)$  и  $(5, 2)^j$  при  $0 \leq j < 6$  образуют систему представителей. 7. Выберем

$u$  и  $v$  таким образом, что  $xv - yu = 1$ . Тогда

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x & u \\ y & v \end{pmatrix} = \begin{pmatrix} m & n \\ n & k \end{pmatrix},$$

где  $n = axu + bxv + byu + cyv$  и  $k = au^2 + 2buv + cv^2$ , дает форму  $mX^2 + 2nXY + kY^2$  с первым коэффициентом  $m$ , собственно эквивалентную данной форме. Таким образом,  $n^2 - D \equiv 0 \pmod{m}$ . Если в процессе из § 8.2 решение  $d$  сравнения  $d^2 \equiv D \pmod{m}$  сравнимо с  $n$  по модулю  $m$ , то формы  $mX^2 + 2nXY + kY^2$  и  $mX^2 + 2dXY + eY^2$  собственно эквивалентны согласно

$$\begin{matrix} n & & -n & & d \\ m & & k & & m & & e \end{matrix}$$

Тогда теорема из этого параграфа показывает, что циклический метод приводит  $mx^2 + 2dxy + ey^2$  и  $ax^2 + 2bxy + cy^2$  к одному периоду и, следовательно, задает явную эквивалентность. 8. Найдите явную эквивалентность данной формы и приведенной формы. Тогда задача состоит в нахождении всех представлений приведенной формой. Используйте метод из § 8.2 для нахождения одного представления (если такое представление существует). Найденные числа можно записать в виде матрицы-столбца, и при  $D > 0$  общее представление равно произведению степени некоторой  $2 \times 2$ -матрицы на полученную матрицу-столбец, причем нужную  $2 \times 2$ -матрицу можно найти в явном виде. 9. (3, 1) не принадлежит главному классу. Метод из упр. 11 к § 5.6 дает  $37^{38} \equiv 43$  как квадратный корень из 37 по модулю 151. Тогда метод из § 8.2 дает  $274^2 - 37 \cdot 45^2 = 151$ .

8.5. 1. См. упр. 6 к § 8.4. 2.  $(2, *) \not\sim I$ ,  $(7, 1)^2 \sim (13, *)$ . Система представителей состоит из дивизоров  $(2, *)^i \cdot (7, 1)^j$  при  $i = 0, 1$ ,  $j = 0, 1, 2, 3$ . 3. Система представителей состоит из дивизоров  $(5, 1)^j$ ,  $0 \leq j < 18$ . Приведенные формы, соответствующие этим степеням, равны (по порядку)  $(1, 0, 531)$ ,  $(5, 3, 108)$ ,  $(25, 12, 27)$ ,  $(17, 8, 35)$ ,  $(7, -1, 76)$ ,  $(20, 7, 29)$ ,  $(4, -1, 133)$ ,  $(20, 3, 27)$ ,  $(19, -1, 28)$ ,  $(9, 0, 59)$ ,  $(19, 1, 28)$ , ... 4.  $(7, 2)^j$  при  $j = 0, 1, 2, 3$  — система представителей. 5.  $(2, 1) \sim (-1, *)$   $(2, 0)$  и  $(2, 1)^j$  при  $j = 0, 1, 2, 3$  — система представителей. 6.  $(5, 1)^j$  при  $0 \leq j \leq 8$  — система представителей. 7.  $(5, 1)^3 \sim I$ . 8.  $(5, 1)^6 \sim I$ . 11. Все формы с детерминантом 5 собственно эквивалентны  $x^2 + 4xy - y^2$ .

8.6. 1. Квадратичный закон взаимности показывает, что  $-5$  является квадратом по модулю  $p$  тогда и только тогда, когда  $p$  сравнимо с 1, 3, 7 или 9 по модулю 20 ( $p \neq 2$  или 5). Пусть  $d^2 \equiv -5 \pmod{p}$  и  $e = (d^2 + 5)/p$ . Эта форма имеет характер  $— —$  и, следовательно, эквивалентна  $2x^2 + 2xy + 3y^2$ . Таким образом,  $p_1$  и  $p_2$  представимы этой формой. Затем примените формулу (2). 2. В действительности предположение о нечетности  $a$  и  $a'$  несущественно, и при  $a = 4$ ,  $b = b' = 0$ ,  $a' = 9$  получается композиция  $(4x^2 + 9y^2) \cdot (9u^2 + 4v^2) = 36X^2 + Y^2$ , где  $X = xu - yv$  и  $Y = 4xv + 9yu$ . Другой способ: класс данной формы соответствует дивизору  $(13, 5)$ ;  $(13, 5)^2$  делит  $(5 - \sqrt{-1})^2$ ,  $12 - 5\sqrt{-1}$ ,  $34 \cdot 12 - 170\sqrt{-1}$ ,  $-99 - \sqrt{-1}$ ,  $82 - \sqrt{-36}$ . Затем циклический метод показывает, что  $(13, 5)^2 \sim I$ .

9.2. 1. При  $D = -6$  и  $-10$  см. табл. 7.8.1. Остаются случаи  $-13$ ,  $-14$  и  $-17$ . Для них воспользуйтесь теоремами Эйлера. 2. Нет.

9.5. 2.  $c_1 = -i/2 = -c_3$ ,  $c_2 = c_4 = 0$ ,  $L(1, \chi) = -(i/2) \log((1+i)/(1-i)) = -i \log \sqrt{i}$ . 3. Пусть  $k=1+\chi(2)2+\chi(3)3+\dots$ . Тогда  $k = -m\Sigma + 2\Sigma'$

и  $k = -m \binom{D}{2} \Sigma + 4 \binom{D}{2} \Sigma'$ . Отсюда  $k = -m \binom{D}{2} \sum [2 \binom{D}{2} - 1]^{-1}$ . Тогда  $h = L(1, \chi) \sqrt{m}/\pi = |\Sigma|$  при  $\binom{D}{2} = 1$  и  $= \frac{1}{3} |\Sigma|$  при  $\binom{D}{2} = -1$  (за исключением случая  $D = -3$ ). 4.  $\binom{-7}{n} = \binom{n}{7}$ ;  $h = |\Sigma| = |1 + 1 - 1| = 1$ ;  $\binom{-11}{n} = \binom{n}{11}$ ;  $h = \frac{1}{3} |\Sigma| = \frac{1}{3} |1 - 1 + 1 + 1 + 1| = 1$ ;  $\binom{-15}{7} = -\binom{-15}{8} = -\binom{-15}{2} = -1$  и  $h = |1 + 1 + 0 + 1 + 0 + 0 - 1| = 2$ ;  $\binom{-19}{7} = -\binom{-19}{12} = -\binom{-19}{3} = +1$  и  $h = \frac{1}{3}$  суммы  $+ - - + + + + - + = 1$ . При  $D = -23, -31, -35, -39, -43, -47$  число классов  $h = 3, 3, 2, 4, 1, 5$  соответственно. 5.  $\binom{D}{1} + \binom{D}{3} 3 + \binom{D}{5} 5 + \dots = \binom{D}{1} [1 - (2D - 1) + (2D + 1) - (4D - 1)] + \binom{D}{3} [3 - (2D - 3) + (2D + 3) - (4D - 3)] + \dots = -4D\Sigma$ . Отсюда  $h = |\Sigma|$ . Искомые числа классов равны 2, 2, 2, 2, 4, 4, 4 соответственно. 6. При  $D = -5$  значения  $\binom{s}{p}$  равны  $+ - - +$  и  $h = 2$ . При  $D = -13$  эти значения равны  $+ - + | + - - | - - + | + - -$  и  $h = 2$ . Остальные числа классов равны 4, 4, 6, 4, 2, 8, 6 соответственно. 7. При  $D = -6$  значение  $s = 1$  лежит в 3-м октанте  $6/8 < s \leq 9/8$  и  $h = 2$ . Другие числа классов равны 4, 2, 4 и 6. 8. Искомые числа классов 2, 6, 4, 4. 9. (a) Если  $\alpha = e^{2\pi i/\lambda}$ , то гауссова сумма равна  $1 + \alpha + \alpha^4 + \alpha^9 + \dots = 1 + 2\theta_0 = \theta_0 - \theta_1$ . (b) Если  $m$  — простое, то  $D \equiv 1 \pmod{4}$  и  $|D|$  — простое число. Таким образом, левая часть (6) равна  $\theta_0 - \theta_1$ . Правая часть равна  $\sqrt{\bar{\lambda}} = \sqrt{\bar{D}} = \sqrt{\bar{m}}$ , если  $D > 0$ , и  $i\sqrt{\bar{\lambda}} = i\sqrt{\bar{m}}$ , если  $D < 0$ . (c)  $i - (-i) = 2i = i\sqrt{4}$ ;  $\sqrt{i} + i\sqrt{i} - (-\sqrt{i}) - (-i\sqrt{i}) = 2\sqrt{i}(1 + i) = 2\sqrt{i}\sqrt{2i} = i\sqrt{m}$ ;  $\sqrt{i} - i\sqrt{i} - (-\sqrt{i}) + (-i\sqrt{i}) = 2\sqrt{i}(1 - i) = \sqrt{m}$ . (d)  $\sum \alpha^k \binom{D}{k} = \sum \alpha^{4a} \times \alpha^{pb} \binom{-1}{4a+pb} \binom{4a+pb}{p} = (\sum \alpha^{pb} \binom{-1}{pb}) (\sum \alpha^{4a} \binom{a}{p}) = \binom{-1}{p} \cdot 2i \cdot \sum \alpha^{4a} \times \binom{-D}{a}$ . Если  $D = p \equiv -1 \pmod{4}$ , то это выражение равно  $(-1) \cdot 2i \times (i\sqrt{p}) = 2\sqrt{p} = \sqrt{m}$ . Если  $D = -p$ , где  $p \equiv 1 \pmod{4}$ , то это выражение равно  $2i\sqrt{p} = i\sqrt{m}$ . (e) Если  $D = 2p$ , то  $\sum \alpha^k \binom{D}{k} = \sum \alpha^{8a+pb} \times \binom{2}{8a+pb} \binom{p}{8a+pb}$ . Если  $p \equiv 1 \pmod{4}$ , то это выражение равно  $\binom{2}{p} \times (\sum \alpha^{pb} \binom{2}{b}) (\sum \alpha^{8a} \binom{8a}{p}) = \sqrt{8} \sum \alpha^{8a} \binom{p}{a} = \sqrt{m}$ . Если  $p \equiv -1 \pmod{4}$ , то это выражение равно

$$\binom{-2}{p} (\sum \alpha^{pb} \binom{-2}{b}) (\sum \alpha^{8a} \binom{8a}{p}) = \binom{-1}{p} i\sqrt{8} \cdot i\sqrt{p} = \sqrt{m}.$$

Доказательство при  $D = -2p$  аналогично. (f) аналогично (e). (g) (6) было выведено из (5) при простом  $n$ . (6) утверждает, что  $m\bar{c}_1 = i\sqrt{m}$  при  $D < 0$ . Таким образом,  $\mu = c_1 = -i\sqrt{m}/m$  определяет знак в (3). Это определяет знак в (4). (h) проверяется непосредственно. (i) Если  $p \equiv -1 \pmod{4}$ , положим  $D = -p$ . Тогда  $h$  или  $3h$  равно  $C_1 + C_2 + C_3 + C_4$  — сумма первой половины символов Лежандра по модулю  $p$ . Если  $p \equiv 1 \pmod{4}$  и  $D = -p$ , то  $h = 2(C_1 + C_2)$  — удвоенная сумма первой четверти символов Лежандра. (j) Знак формулы для числа классов определяет знак гауссовой суммы.

9.6. 1. См. упр. 5 к § 8.4. 2. Используя (3), получаем  $h = 1 \cdot \frac{1}{3} \cdot 6 \cdot (1 + \frac{1}{2}) \times (1 - \frac{1}{3}) = 2$ ;  $I$  и  $(-1, *)$  образуют систему представителей. 3. Так

как  $t = 2$ , то  $h_0$  умножается на  $2 - \binom{D}{p}$ , что и требовалось показать. Это правило годится и для  $D = -3$ .

9.7. 6. Пусть  $a$  — произведение  $\mu_i$ -х степеней  $p_i$ ,  $i = 1, 2, \dots, n$ . Вещественные характеры по модулю  $a$  имеют вид  $\chi_1 \chi_2 \dots \chi_n$ , где характер  $\chi_i$ , соответствующий  $p_i$ , либо является главным характером по модулю  $p_i$ , либо символом Лежандра по модулю  $p_i$  (если  $p_i \neq 2$ ), либо одним из 4 вещественных характеров по модулю 8 (если  $p_i = 2$ ). Поэтому его можно записать в виде

$$\chi(n) = \binom{\varepsilon}{n} \binom{r}{n} \binom{n}{q_1} \binom{n}{q_2} \dots \binom{n}{q_p} \binom{n}{q'_1} \binom{n}{q'_2} \dots \binom{n}{q'_s},$$

где  $q_i$  — простые из числа  $p_i$ , сравнимые с 1 по модулю 4,  $q'_i$  — простые из числа  $p_i$ , сравнимые с  $-1$  по модулю 4,  $\varepsilon = \pm 1$  и  $r = 1$  или 2, за тем исключением, что  $\chi(n) = 0$  при  $n$ , делящемся на одно из чисел  $p_i$ , тогда как правая часть равна нулю, только если  $n$  делится на одно из чисел  $q_i$  или  $q'_i$ . Правая часть равна  $\binom{D}{n}$ , где  $D = \varepsilon r q_1 q_2 \dots q_p (-q'_1) (-q'_2) \dots (-q'_s)$  (см. § 7.8). Таким образом,

$$L(s, \chi) = \prod (1 - \chi(p) p^{-s})^{-1} = (1 - \chi(r_1) r_1^{-s}) \dots (1 - \chi(r_t) r_t^{-s}) L(s, \chi_D),$$

где  $r$  — числа  $p$ , отличные от  $q$ .

А.1. 1. Если  $a = a'd$  и  $b = b'd$ , то  $qa + rb = (qa' + rb')d$ . 2. Если  $a = ub$  и  $b = va$ , то  $a = uva = 1 \cdot a$  и  $uv = 1$ . Если  $u > 1$ , то  $1 = uv > v \geq 1$ , что невозможно. Следовательно,  $a = 1 \cdot b = b$ . 3. Пусть  $a = a_0$ ,  $b = a_1$ ,  $a_{i+1} = q_i a_i + a_{i-1}$ ,  $a_0 > a_1 > \dots > a_n = d$ . Тогда  $a_{n-2} = q_{n-1} a_{n-1} + d$ . Если  $ua_i = d + va_{i+1}$ , то  $ua_i + q_i va_i = d + v(q_i a_i + a_{i+1})$ ,  $Ua_i = d + va_{i-1}$ , а если  $ua_i + d = va_{i+1}$ , то  $Ua_i + d = va_{i-1}$ , где  $U = u + q_i v$ . Если  $ax + 1 \equiv 0 \pmod{b}$ , то  $a^2 x^2 + 2ax + 1 \equiv 0 \pmod{b}$ ,  $a^2 x^2 + 2(ax + 1) \equiv 1 \pmod{b}$ ,  $Ax \equiv 1 \pmod{b}$ , где  $A = a^2 x$ . Если  $a$  и  $b$  взаимно просты, то система  $y (= ax) \equiv 0 \pmod{a}$ ,  $y \equiv 1 \pmod{b}$  имеет решение. По симметрии, система  $z \equiv 1 \pmod{a}$ ,  $z \equiv 0 \pmod{b}$  имеет решение. Значит, число  $u = cz + dy$  удовлетворяет системе  $u \equiv c \pmod{a}$ ,  $u \equiv d \pmod{b}$ , как это и требуется. 4. (a) решений нет. (b)  $x = 2 + 5k \equiv 3 \pmod{7}$ ,  $8 + 20k \equiv 12 \pmod{7}$ ,  $1 \equiv 5 + k \pmod{7}$ ,  $3 \equiv k \pmod{7}$ ,  $k = 3 + 7n$ ,  $x = 17 + 35n$ . (c)  $x = 2 + 295k$ ,  $7 \equiv 2 + 15k \pmod{56}$ ,  $1 \equiv 3k \pmod{56}$ ,  $19 \equiv 57k \pmod{56}$ ,  $x = 5607 + 56 \cdot 295n$ . 5. См. выше упр. 3. 6. Найдем такие  $b_2, b_3, \dots, b_n$ , чтобы  $b_i \equiv 1 \pmod{c_1}$ ,  $b_i \equiv 0 \pmod{c_i}$ . Положим  $d_1 = b_2 b_3 \dots b_n$ . Тогда  $d_1 \equiv 1 \pmod{c_1}$ ,  $d_1 \equiv 0 \pmod{c_i}$  для  $i = 2, 3, \dots, n$ . Этим же способом найдем такое  $d_i$ , чтобы  $d_i \equiv 1 \pmod{c_i}$ ,  $d_i \equiv 0 \pmod{c_j}$  ( $j \neq i$ ). Число  $a_1 d_1 + a_2 d_2 + \dots + a_n d_n$  удовлетворяет данной задаче. 7. Если  $a$  отрицательно, то положим  $ax = (-a)(-x)$ . Пусть  $d$  — наибольший общий делитель чисел  $a$  и  $b$ . На основании упр. 3  $d = ua + vb$  при целых  $u$  и  $v$ . Если  $c$  не делится на  $d$ , то ясно, что решения нет. Если  $c = qd$ , то  $x = -qu$ ,  $y = -qv$  образуют решение. Если  $X, Y$  — частное решение, то самое общее решение имеет вид  $x = X + r$ ,  $y = Y + s$ , где  $ar + bs = 0$ . Это равносильно условию  $a'r + b's = 0$ , где  $a = a'd$ ,  $b = b'd$ . Для любого решения этого уравнения мы имеем  $a'r \equiv 0 \pmod{b'}$ ,  $r \equiv 0 \pmod{b'}$  ( $b'$  и  $a'$  взаимно просты),  $r = kb'$ ,  $s = -kb'a'/b' = -ka'$ . Таким образом, наиболее общим решением является  $x = -qu + kb'$ ,  $y = -qv - ka'$ .

А.2. 2. Сравнение  $\gamma^a \equiv \gamma^b \pmod{p}$  равносильно сравнению  $a \equiv b \pmod{p-1}$ . Если  $k$  взаимно просто с  $p-1$ , то  $(\gamma^k)^a \equiv 1 \pmod{p}$  только в том случае, когда  $p-1$  делит  $a$  и  $\gamma^k$  — примитивный корень по модулю  $p$ . Обратно, если  $\gamma^k$  — примитивный корень, то  $\gamma \equiv (\gamma^k)^a$  при некотором  $a$ ,  $ak \equiv 1 \pmod{p-1}$  и  $k$  взаимно просто с  $p-1$ .

## ЛИТЕРАТУРА <sup>1</sup>

- [A1] Comptes Rendus de l'Académie des Sciences, Paris, vol. 24 (1847), p. 310 et seq. 96.
- [B1] Bell E. T., The Last Problem, Simon and Schuster, New York, 1961. 39.
- [B2] Борович З. И., Шафаревич И. Р. Теория чисел.— М.: Наука, 1964. 277, 289.
- [B3] Bourbaki N., Élements d'Histoire des Mathématiques, 2-ème éd., Hermann, Paris, 1969. [Имеется перевод 1-го изд.: Бурбаки Н. Очерки по истории математики.— М.: ИЛ, 1963.] 296.
- [C1] Cayley A., Tables des formes quadratiques binaires, *Jour. für Math.* (Crelle), 60 (1862), 357—372 (Mathematical Papers, vol. 5, Cambridge, 1892, Johnson Reprint Corp., New York and London, 141—156). 396.
- [C2] Cohn H., A Second Course in Number Theory, Wiley, New York and London, 1962. 396.
- [C3] Colebrooke H. T., Algebra with Arithmetic and Mensuration from the Sanskrit of Brahmegeupta and Bhaskara, London, 1817. 44.
- [D1] Dedekind R., см. [D7].
- [D2] Dickson L. E., History of the Theory of Numbers (3 vols.), Carnegie Institute of Washington, 1919, 1920, and 1923 (reprint, Chelsea Pub. Co., New York, 1971). 24, 25, 27, 43, 54, 62, 90, 95, 371, 442.
- [D3] Diophanti Alexandrini arithmeti corum libri sex, et de numeris multangulis liber unus. Cum commentariis C. G. Bacheti V. C. et observationibus D. P. de Fermat Senatoris Tolosani, Toulouse, 1670. [Имеется перевод: Диофант. Арифметика и книга о многоугольных числах.— М.: Наука, 1974.] 14.
- [D4] Dirichlet P.G.L., Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. *Jour. für Math.* (Crelle) 3 (1828), 354-375 (Werke, vol. 1, 21-46).
- [D5] Dirichlet P.G.L., Démonstration du théorème de Fermat pour le cas des 14ièmes puissances, *Jour. für Math.* (Crelle) 9 (1832), 390-393 (Werke, vol. 1, 189-194). 94.
- [D6] Dirichlet P.G.L., Über eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen, *Abh. Königl. Preuss. Akad. Wiss.*, 1835, 391-407. 425.
- [D7] Dirichlet P.G.L., Vorlesungen über Zahlentheorie, herausgegeben und mit Zusätzen versehen von R. Dedekind, Vieweg und Sohn, Braunschweig, 1893 (reprint Chelsea Pub. Co., New York, 1968). [Имеется перевод: Дирихле Петер Густав Лежен. Лекции по теории чисел в обработке и с добавлением Р. Дедекинда.— М.—Л.: ОНТИ НКТП СССР, 1936.] 367, 388, 407, 424, 425, 431.
- [E1] Edwards H. M., Advanced Calculus, Houghton Mifflin, Boston, 1969. 172, 257.

---

<sup>1</sup>) Выделенные жирным шрифтом цифры указывают страницы этой книги, где цитируются соответствующие источники.



- [E2] Edwards H. M., Riemann's Zeta Function, Academic Press, New York, 1974.
- [E3] Edwards H. M., The background of Kummer's proof of Fermat's Last Theorem for regular primes, *Arch. Hist. Exact. Sci.*, 14 (1975), 219-236. 101, 155.
- [E4] Edwards H. M., Postscript to «The background of Kummer's proof of Fermat's Last Theorem for regular primes» (to appear). 101, 119.
- [E5] Euclid, Elements, T. L. Heath, ed., Cambridge Univ. Press, New York, 1908, 3 vols. (reprint Dover, New York, 1956). [Имеется перевод: Евклид, Начала Евклида.— М.—Л.: Гостехтеориздат, 1950.]
- [E6] Euler L., Introductio in Analysin Infinitorum, Bousquet et Socios., Lausanne, 1748 (Opera (1), vol. 8). [Имеется перевод: Эйлер Леонард, Введение в анализ бесконечных.— М.: Физматгиз, 1961.] 416.
- [E7] Euler L., Theoremata circa divisores numerorum in hac forma  $paa \pm qbb$  contentorum, *Comm. Acad. Sci. Petrop.* 14 (1751), 151-181; Opera (1), 2, 194-222. 340.
- [E8] Euler L., De numeris, qui sunt aggregata duorum quadratorum, *Nov. Comm. Acad. Sci. Petrop.* 4 (1758), 3-40; Opera (1), 2, 295-327. 64.
- [E9] Euler L., Vollständige Anleitung zur Algebra, СПб., 1770; Opera (1), vol. I. 50, 61.
- [E10] Euler L., Extrait d'une lettre de M. Euler à M. Beguelin en mai 1778, *Nouv. Mém. Acad. Sci. Berlin*, 1776, 1779, 337-339; Opera (1), 3, 418-420. 370.
- [E11] Euler L., Observationes circa divisionem quadratorum per numeros primos, *Opuscula Analytica*, 1 (1783), 64-84; Opera (1), 3, 497-512. 341.
- [E12] Euler L., Opera (1), 4, Vorwort des Herausgebers (III. Grosse Primzahlen) and related papers 708, 715, 718, 719, and 725 of Euler. 370, 371.
- [F1] de Fermat P., Oeuvres, 3 vols., Gauthier-Villars, Paris, 1891, 1894, 1896.
- [F2] de Fermat P., Observations on Diophantus, originally published in [D3]; also [F1], 1, 291-342; French transl. [F1], 3, 241-274.
- [F3] de Fermat P., Letter to Pascal, 25 Sept. 1654. Oeuvres de Pascal, 4, 437-441; also [F1], 2, 310-314. 74.
- [F4] de Fermat P., Letter to Digby, sent by Digby to Wallis on 19 June 1658, published by Wallis in [W3]; republished [W2] and [F1], 2, 402-408; French transl. [F1], 3, 314-319. 66.
- [F5] de Fermat P., Letter to Carcavi, dated August 1659, [F1], 2, 431-436. 39, 75.
- [F6] Fuss P.-H., ed., Correspondance Mathématique et Physique, Имп. Академия наук, СПб., 1843, vol. 1 (reprint, Johnson Reprint Corp., New York and London, 1968). 63, 64, 340.
- [G1] Gauss C. F., Disquisitiones Arithmeticae, Leipzig, 1801; republished, 1863, as vol. 1 of Werke; French transl., Recherches Arithmétiques, Paris, 1807; republished, Hermann, Paris, 1910; German transl. in [G2]; English transl., Yale, New Haven and London, 1966. [Имеется перевод: Гаусс Карл Фридрих. Труды по теории чисел.— М.: Изд-во Акад. наук СССР, 1959.]
- [G2] Gauss C. F., Untersuchungen über Höhere Arithmetik (German transl. of [G1] and other works on number theory) H. Maser, transl., Springer-Verlag, Berlin, 1889 (reprint, Chelsea Pub. Co., New York, 1965). 394, 410.
- [G3] Gauss C. F., Theorematis arithmetici demonstratio nova, *Comm. Soc. Reg. Sci. Gott.*, 16 (1808); Werke, 2, 3-8; German transl. in [G2]. 341, 359.
- [G4] Gauss C. F., Summatio quarundam serierum singularium, *Comm. Soc. Reg. Sci. Gott. Rec.* 1 (1811); Werke, 2, 11-45; German transl. in [G2]. 425, 426.

- [G5] Gauss C. F., Theorematis fundamentalis in doctrina de residuis quadratici demonstrationes et ampliaciones novae, *Comm. Soc. Reg. Sci. Gott. Rec.* 4 (1818); Werke, 2, 49-64; German transl. in [G2]. 208.
- [G6] Gauss C. F., Theoria residuorum biquadraticorum, Commentatio prima, *Comm. Soc. Reg. Sci. Gott. Rec.* 6 (1828), Commentatio secunda, 7 (1832); Werke, 2, 67-148; German transl. in [G2]. 107.
- [G7] Gauss C. F., De nexu inter multitudinem classium, in quas formae binae secundum gradum distribuuntur, earumque determinantem, commentatio prior Societati Regiae exhibita, 1834; Werke, 2, 269-303; German transl. in [G2].
- [G8] Gauss C. F., Letter to Sophie Germain, Werke, 10 (part 1), 70-73; also in *Oeuvres Philosophiques de Sophie Germain*, Paris, 1896, p. 275. 80.
- [G9] Grube F., Über einige Eulersche Sätze aus der Theorie der quadratischen Formen, *Zeitschr. Math. Phys.*, 19 (1874), 492-519. 371.
- [H1] Heath T. L., Diophantus of Alexandria, Cambridge University Press, 1910 (reprint, Dover, New York, 1964). 17, 26, 29, 42, 44.
- [H2] Hecke E., Vorlesungen über die Theorie der Algebraischen Zahlen, Akad. Verlag, Leipzig, 1923 (reprint, Chelsea Pub. Co., New York, 1948). [Имеется перевод: Гекке Эрик. Лекции по теории алгебраических чисел. М.—Л.: Гостехиздат, 1940.] 208.
- [H3] Hilbert D., Die Theorie der algebraischen Zahlkörper (called «the Zahlbericht»), *Jahresber. der Deut. Math. Verein*, 4 (1897), 175-546; *Gesammelte Abhandlungen*, 1, 63-363. 206.
- [I1] Ince E. L., Cycles of Reduced Ideals in Quadratic Fields, Brit. Assn. for the Advancement of Science, Mathematical Tables, vol. 4, Camb. Univ. Press, New York 1966. 396.
- [J1] Jacobi C. G. J., Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie, *Monatsber. Akad. Wiss. Berlin*, 1837, 127-136; also *Jour. für Math.* (Crelle) 30 (1846), 166-182; and Werke, 6, 254-274. 77. 345.
- [J2] Jacobi C. G. J., Über die complexen Primzahlen, welche in der theorie der Reste der 5ten, 8ten, und 12ten Potenzen zu betrachten sind, *Monatsber. der Akad. Wiss. Berlin*, 1839, 86-91; also *Jour. für Math.* (Crelle) 19 (1839), 314-318; and Werke, 6, 275-280; French transl., *Jour. de Math.*, 8 (1843), 268-272. 100, 111.
- [J3] Jacobi C. G. J., Canon Arithmeticus, Akademie-Verlag, Berlin, 1956 (originally published by Typis Academicus Berolini, 1839). 447.
- [J4] Johnson W., Irregular primes and cyclotomic invariants, *Math. of Computation*, 29 (1975), 113-120. 289.
- [K1a] Kline M., Mathematical Thought from Ancient to Modern Times, Oxford, New York, 1972. 41.
- [K1] Kronecker L., Zur Geschichte des Reciprocitätsgesetzes, *Monatsber. Akad. Wiss. Berlin*, 1875, 267-274; Werke, vol. 2, 1-10. 346.
- [K2] Kronecker L., Ein Fundamentalsatz der allgemeinen Arithmetik, *Jour. für Math.* (Crelle) 100 (1887), 490-510; Werke, vol. 3, 211-240. 107.
- [K3] Kronecker L., Über den Zahlbegriff, *Jour. für Math.* (Crelle) 101 (1887), 337-355; Werke, vol. 3, 251-274. 107.
- [K4] Kummer E. E., Collected Papers, André Weil, ed., vol. I, Contributions to Number Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1975.
- [K5] Festschrift zur Feier des 100. Geburtstages Eduard Kummers, Abh. Gesch. Math. Wiss., Teubner, Berlin and Leipzig, 1910; reprint, [K4], 31-133. 398.
- [K6] Kummer E. E., De numeris complexis, qui radicibus unitatis et numeris integris realibus constant, Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg; reprint, *Jour. de Math.*, 12 (1847), 185-212, and [K4], 165-192. 99, 125.
- [K7] Kummer E. E., Zur Theorie der Complexen Zahlen, *Monatsber. Akad.*

*Wiss. Berlin*, 1846, 87-96; also *Jour. für Math. (Crelle)* 35 (1847), 319-326, and [K4], 203-210. 99, 172, 182, 398.

- [K8] Kummer E. E., Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren, *Jour. für Math. (Crelle)* 35 (1847), 327-367; also [K4], 211-251. 99, 155, 171, 172, 183, 296.
- [K9] Kummer E. E., Extrait d'une lettre de M. Kummer à M. Liouville, *Jour. de Math.*, 12 (1847), p. 136; also [K4], p. 298.
- [K10] Kummer E. E., Beweis des Fermat'schen Satzes der Unmöglichkeit von  $x^\lambda + y^\lambda = z^\lambda$  für eine unendliche [sic] Anzahl Primzahlen  $\lambda$ , *Monatsber. Akad. Wiss. Berlin*, 1847, 132-141, 305-319; also [K4], 274-297. 216.
- [K11] Kummer E. E., Bestimmung der Anzahl nicht äquivalenter Classen für die aus  $\lambda$ ten Wurzeln der Einheit gebildeten complexen Zahlen, *Jour. für Math. (Crelle)* 40 (1850), 93-116; also [K4], 299-322. 183, 296.
- [K12] Kummer E. E., Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus  $\lambda$ ten Wurzeln der Einheit gebildeten complexen Zahlen, *Jour. für Math. (Crelle)* 40 (1850), 117-129; also [K4], 323-335.
- [K13] Kummer E. E., Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung  $x^\lambda + y^\lambda = z^\lambda$  durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten  $\lambda$ , welche ungerade Primzahlen sind und in den Zählern der ersten  $(\lambda-3)/2$  Bernoulli'schen Zahlen als Factoren nicht vorkommen, *Jour. für Math. (Crelle)* 40 (1850), 130-138; also [K4], 336-344.
- [K14] Kummer E. E., Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers, *Jour. de Math.* 16 (1851), 377-498; also [K4], 363-484. 269, 276.
- [K15] Kummer E. E., Über die Irregularität von Determinanten, *Monatsber. Akad. Wiss. Berlin*, 1853, 194-200; also [K4], 539-545. 269.
- [K16] Kummer E. E., Über die den Gaussischen Perioden der Kreistheilung entsprechenden Congruenzwurzeln, *Jour. für Math. (Crelle)* 53 (1857), 142-148; also [K4], 574-580. 155.
- [K17] Kummer E. E., Über diejenigen Primzahlen  $\lambda$ , für welche die Klassenzahl der aus  $\lambda$ ten Einheitswurzeln gebildeten complexen Zahlen durch  $\lambda$  teilbar ist, *Monatsber. Akad. Wiss. Berlin*, 1874, 239-248; also [K4], 945-954. 269.
- [L1] Lagrange J. L., Sur la solution des problèmes indéterminés du second degré, *Mém. de l'Acad. Roy. Sci. et Belles-Lettres*, Berlin, 23 (1769) (*Oeuvres*, 2, 377-535). 215, 403.
- [L2] Lagrange J. L., Additions to Euler's *Algebra*. First published 1774, Lyon, in vol. 2 of a French translation of Euler's *Algebra* [E9]; republished in vol. 7 of Lagrange's *Oeuvres*, 5-180, and in vol. (1) 1 of Euler's *Opera*. 354.
- [L3] Lagrange J. L., *Oeuvres*, vol. 2, Paris, 1868, 531-535. 97.
- [L4] Lagrange J. L., *Oeuvres*, vol. 14, Paris, 1892, 298-299. 79.
- [L5] Lamé G., Démonstration général du théorème de Fermat, *Comptes Rendus*, 24 (1847), 310-315.
- [L6] Lamé G., Mémoire sur la résolution, en nombres complexes, de l'équation  $A^5 + B^5 + C^5 = 0$ , *Jour. de Math.* 12 (1847), 137-184. 121.
- [L7] Legendre A. M., Sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat, *Mém. Acad. R. Sc. de l'Institut de France*, 6, Paris 1827; also appeared as 2nd Supplement to 1808 edition of [L8]. 81, 90.
- [L8] Legendre A. M., *Théorie des Nombres*, vol. 2, Paris, 1830, pp. 361-368 (reprint, Blanchard, Paris, 1955).
- [M1] Mordell L. J., On a simple summation of the series  $\sum e^{2s^2\pi i/n}$ , *Messenger of Math.*, 48 (1919), 54-56. 425.

- [N1] Neugebauer O., The Exact Sciences in Antiquity, Brown University Press, Providence, 1957, Chapter 2. 17.
- [N2] Newton I., The Correspondence of Isaac Newton, vol. 2, H. W. Turnbull, ed., Cambridge, 1960, 110-160. 410.
- [N3] Nörlund N. E., Differenzenrechnung, Springer-Verlag, Berlin, 1924.
- [O1] Ohm M., Etwas über die Bernoullischen Zahlen. *Jour. für Math.* (Crelle) 20 (1840), 11-12. 274.
- [S1] Shanks D., Five Number-theoretic Algorithms, Proceedings of the 2nd Manitoba Conference on Numerical Mathematics, 51-70, Univ. of Manitoba, Winnipeg, 1972. 215.
- [S2] Smith D. E., A Source Book in Mathematics, McGraw-Hill, New York, 1929 (reprint, Dover, New York, 1959). 99.
- [S3] Smith H. J. S., Report on the Theory of Numbers, originally published in six parts as a Report of the British Assn; reprinted, 1894, in The Collected Mathematical Papers of H. J. S. Smith; (reprinted, both separately and as part of the Mathematical Papers, Chelsea Pub. Co., New York, 1965). 48, 101, 276, 340, 359, 425.
- [S4] Steinig J., On Euler's idoneal numbers, *Elemente der Math.*, 21 (1966) 73-88. 370.
- [T1] Toeplitz O., Die Entwicklung der Infinitesimal Rechnung, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1949; English transl. The Calculus: A Genetic Approach, Univ. of Chicago, Chicago, 1963. 9.
- [W1] Wagstaff S., Fermat's Last Theorem is true for any exponent less than 1 000 000 (Abstract), *AMS Notices*, No. 167 (1976) p. A-53. 289.
- [W2] Wallis J., Opera Mathematica, 3 vols., Oxford, 1695-1699 (reprint, G. Olms, Hildesheim-New York, 1972).
- [W3] Wallis J., ed., Commercium Epistolicum, Oxford, 1658 (reprint, [W2]; French transl., [F1]).
- [W4] Weil A., La cyclotomie jadis et naguère, *L'Enseignement Mathématique* (2) 20 (1974), 247-263. 425.

## УКАЗАТЕЛЬ

Аналитический метод 18, 111, 115, 138, 291

Баше 14

— комментарий к Диофанту 25

*Бернулли* полиномы 273

— числа 273—274

Бесконечного спуска метод 21—22, 440

Бинарные квадратичные формы 373

Брахмагупта 44

Броункер 48

Бхаскара Акхария 44, 48

Валлис 48—50

Гаусс 79

Гауссовы суммы 426

Группа классов дивизоров порядка квадратичных целых 368

Двусторонние классы дивизоров 355—358

Дедекиндр 173

Деление для круговых целых 106

Дзета-функция 220

Дивизор для квадратичных целых 303—304

— для круговых целых 168

Диксон 27

Диофант 43

Дирихле 85, 94

*Евклида* алгоритм 440—441

— формула для совершенных чисел 34

Единица 84

*Жермен Софи* теорема 83

*Жирара* теорема 29—30

Идеал 174

Идеальные простые делители *см.*

Простые дивизоры

Индекс порядка квадратичных целых 367

Квадратичные целые 297

Квадратичный закон взаимности 209—211, 213, 214, 340, 341, 344, 345—347, 360—362

Китайская теорема об остатках 442

— — — для дивизоров 177

Композиция форм 397—402

Конечность числа классов 195—197

Коши 97—99

Кратности 163, 169

Кronecker 107, 208, 346

Круговые целые 102

*Куммера* лемма 287

Лагранж 49, 69, 78

*Лагранжа* контрпример к гипотезе Эйлера 354—355

Ламе 94, 96—99

Лежандр 79, 85, 90

*Лежандра* символ 212, 344

*Лейбница* формула 410, 421, 423

Лиувилль 97

*Мерсенна* простые 35

Непрерывные дроби 331, 372

Неразложимые круговые целые 105

Норма дивизора 175—176, 305—306

— квадратичного целого 292

— кругового целого 104

Однозначность разложения на простые, отсутствие однозначности 37, 444

Основная единица порядка квадратичных целых 321, 322, 392  
 — теорема арифметики 444  
 — — теории дивизоров 166

Пелль 50

Периоды 132

Порядки квадратичных целых 367

Представление числа формами 373—377

Примитивные бинарные квадратичные формы 382

— корни 446—447

Приведенные дивизоры 330

Простые дивизоры 131, 153, 165, 293—298

— круговые целые 105

Разветвление простых 298

Распадающиеся классы 342

Распадение простых 298

Регулярности критерий 289

Регулярные простые 201

*Римана* дзета-функция 221

Род класса дивизоров 352, 397

Система представителей 195, 323

Собственная эквивалентность квадратичных форм 380, 400

Собственно примитивные бинарные квадратичные формы 382

Собственные представления 377

Сопряжение круговых целых 132

Сопряженные кругового целого 109

Сравнение по модулю дивизора 172—173

— — — кругового целого 107, 112

— — — простого дивизора 153

Сравнения для натуральных чисел 441

Суммирование по частям 226, 229

Теория полей классов 342 (прим.)

Удобные числа 354, 369—371

Формула для числа классов 268, 410, 414, 416, 430

Ферма 13—15

— вызов англичанам 41—42

— открытия в теории чисел 53—55

— Последняя теорема 14—15

— теорема 49

— числа 39—41

*Фурье* анализ (конечномерный) 247

Характер дивизора 350

— класса дивизоров 350, 397

Характеры по модулю простого числа 224

— — — целого числа 433

Циклические матрицы 247

Циклический метод 44—48, 315

Число классов 195, 250, 255, 268

Эквивалентность бинарных квадратичных форм 374

— дивизоров 194, 304, 367

— единиц 254

*Якоби* символ 345



# ОГЛАВЛЕНИЕ

От редактора перевода . . . . .	5
Предисловие . . . . .	7
ГЛАВА 1. ФЕРМА . . . . .	13

**1.1. Ферма и его «Последняя теорема».** Формулировка теоремы. История ее открытия. **1.2. Пифагоровы треугольники.** Пифагоровы тройки, которые были известны вавилонянам за 1000 лет до Пифагора. **1.3. Как находить пифагоровы тройки.** Метод, основанный на том, что произведение двух взаимно простых чисел может быть квадратом только тогда, когда оба сомножителя являются квадратами. **1.4. Метод бесконечного спуска.** **1.5. Случай  $n = 4$  Последней теоремы.** В этом случае доказательство состоит в применении бесконечного спуска. Общая теорема сводится к случаю простых показателей. **1.6. Одно доказательство Ферма.** Доказательство того, что пифагоров треугольник не может иметь площадь, равную квадрату, включает элементарные, но очень остроумные соображения. **1.7. Суммы двух квадратов и родственные вопросы.** Открытия Ферма, относящиеся к представлениям чисел в виде  $n = x^2 + ky^2$  при  $k = 1, 2, 3$ . Отличие в случае  $k = 5$ . **1.8. Совершенные числа и теорема Ферма.** Формула Евклида для совершенных чисел приводит к изучению простых Мерсенна  $2^n - 1$ , которое в свою очередь ведет к теореме Ферма  $a^p - a \equiv 0 \pmod{p}$ . Доказательство теоремы Ферма. Числа Ферма. Ошибочное предположение о простоте числа  $2^{32} + 1$ . **1.9. Уравнение Пелля.** Вызов Ферма англичанам. Циклический метод, изобретенный древними индийцами для решения уравнения  $Ax^2 + 1 = y^2$  при данном  $A$ , не равном квадрату. Эйлер ошибочно назвал это уравнение «уравнением Пелля». Упражнения: доказательство того, что уравнение Пелля имеет бесконечное число решений и что циклический метод дает все такие решения. **1.10. Другие открытия Ферма в теории чисел.** Наследие Ферма, которое осталось в виде задач, предложенных им в качестве вызова. Решения этих задач, данные Лагранжем, Эйлером, Гауссом, Коши и другими.

ГЛАВА 2. ЭЙЛЕР . . . . .	56
--------------------------	----

**2.1. Эйлер и Последняя теорема Ферма при  $n = 3$ .** Эйлер не опубликовал правильного доказательства неразрешимости уравнения  $x^3 + y^3 = z^3$ , однако эту теорему можно доказать, используя его методы. **2.2. Доказательство Эйлера для  $n = 3$ .** Сведение Последней теоремы Ферма в случае  $n = 3$  к утверждению, что  $p^2 + 3q^2$  только тогда может быть кубом ( $p$  и  $q$  — взаимно простые), когда существуют такие  $a$  и  $b$ , что  $p = a^3 - 9ab^2$ ,  $q = 3a^2b - 3b^3$ . **2.3. Арифметика иррациональных чисел.** Условие  $p^2 + 3q^2 =$  куб можно записать просто в виде  $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$ , т. е.  $p + q\sqrt{-3}$  является кубом. Ошибочное доказательство Эйлера, использующее однозначность разложения

на множители, необходимость этого условия для того, чтобы  $p^2 + 3q^2$  было равно кубу. **2.4. Эйлер о суммах двух квадратов.** Эйлеровы доказательства основных теорем о представлениях чисел в виде  $x^2 + y^2$  и  $x^2 + 3y^2$ . Упражнения: числа вида  $x^2 + 2y^2$ . **2.5. Завершение доказательства Последней теоремы Ферма при  $n = 3$ .** Использование методов Эйлера для доказательства неразрешимости уравнения  $x^3 + y^3 = z^3$ . **2.6. Дополнение о суммах двух квадратов.** Метод решения уравнения  $p = x^2 + y^2$  при простом  $p$  вида  $4n + 1$ . Решение уравнений  $p = x^2 + 3y^2$  и  $p = x^2 + 2y^2$ .

## ГЛАВА 3. ОТ ЭЙЛЕРА ДО КУММЕРА . . . . .

78

**3.1. Введение.** Лагранж, Лежандр и Гаусс. **3.2. Теорема Софи Жермен.** Софи Жермен. Разделение Последней теоремы Ферма на два случая, случай I ( $x, y, z$  взаимно просты с показателем  $p$ ) и случай II (когда это не так). Теорема Софи Жермен — достаточное условие для случая I. Оно дает легкое доказательство случая I для всех небольших простых показателей. **3.3. Случай  $n = 5$ .** Доказательство того, что  $x^5 + y^5 \neq z^5$ . Совместное достижение Дирихле и Лежандра. Общая техника подобна эйлерову доказательству утверждения  $x^3 + y^3 \neq z^3$ , за исключением того, что из равенства выражения  $p^2 - 5q^2$  пятой степени вытекает равенство  $p + q\sqrt{5} = (a + b\sqrt{5})^5$  только при дополнительном условии  $5 \mid q$ . **3.4. Случай  $n = 14$  и  $n = 7$ .** Доказательства, полученные соответственно Дирихле и Ламе, здесь не приводятся. Для того чтобы продвинуться дальше и доказать Последнюю теорему Ферма для больших показателей, очевидно, требуется новая техника. Упражнение: данное Дирихле доказательство случая  $n = 14$ .

## ГЛАВА 4. КУММЕРОВА ТЕОРИЯ ИДЕАЛЬНЫХ ДЕЛИТЕЛЕЙ

96

**4.1. События 1847 года.** «Доказательство» Ламе Последней теоремы Ферма. Возражение Лиувилля. Попытки доказательства, предпринятые Коши. Письмо Куммера Лиувиллю. Нарушение однозначности разложения. Новая теория Куммера идеальных комплексных чисел. **4.2. Круговые целые.** Основные определения и действия. Норма кругового целого. Различие между «простым» и «неразложимым». Деление с использованием нормы. **4.3. Разложение простых чисел  $p \equiv 1 \pmod{\lambda}$ .** Получение необходимых и достаточных условий того, что круговое целое является простым делителем такого простого  $p$ . **4.4. Вычисления для  $p \equiv 1 \pmod{\lambda}$ .** Явные разложения таких простых при малых значениях  $p$  и  $\lambda$ . Разложения Куммера при  $\lambda \leq 19$  и  $p \leq 1000$ . Невозможность разложения, когда  $\lambda = 23$  и  $p = 47$ . Идея, лежащая в основе «идеальных» простых делителей Куммера. **4.5. Периоды.** Сопряжение  $\sigma: \alpha \mapsto \alpha^\lambda$ , соответствующее примитивному корню  $\gamma$  по модулю  $\lambda$ . Круговое целое тогда и только тогда образовано периодами длины  $f$ , когда оно инвариантно относительно  $\sigma^e$ , где  $ef = \lambda - 1$ . **4.6. Разложение простых  $p \not\equiv 1 \pmod{\lambda}$ .** Если  $f$  — показатель числа  $p$  по модулю  $\lambda$  и если  $h(\alpha)$  — любой простой делитель числа  $p$ , то все периоды длины  $f$  сравнимы с целыми числами по модулю  $h(\alpha)$ . Это позволяет легко проверять делимость круговых целых, образованных периодами, на  $h(\alpha)$ . **4.7. Вычисления при  $p \not\equiv 1 \pmod{\lambda}$ .** Явные разложения для малых значений  $p$  и  $\lambda$ . **4.8. Расширение признака делимости.** Проверка делимости произвольного кругового целого — не обязательно образованного периодами — на данное простое круговое целое  $h(\lambda)$ . **4.9. Простые дивизоры.** Признаки делимости на простые дели-

тели существуют во всех случаях, даже в тех, когда простого делителя вообще нет. Это является основой определения «идеального» простого делителя, или простого дивизора. Дефект в первоначальном доказательстве Куммера основного предложения.

**4.10. Кратности и исключительное простое число.** Определение кратности, с которой простой дивизор делит круговое целое. Один простой дивизор  $(1 - \alpha)$  числа  $\lambda$ .

**4.11. Основная теорема.** Круговое целое  $g(\alpha)$  тогда и только тогда делит другое  $h(\alpha)$ , когда каждый простой дивизор, делящий  $g(\alpha)$ , делит  $h(\alpha)$  с меньшей или, в крайнем случае, такой же кратностью.

**4.12. Дивизоры.** Определение дивизоров. Обозначение.

**4.13. Терминология.** Дивизор определен множеством всех объектов, которые он делит. «Идеалы».

**4.14. Сопряжения и норма дивизора.** Сопряженные дивизора. Норма дивизора как дивизор и как целое число. Имеется  $N(A)$  классов круговых целых по модулю  $A$ . Китайская теорема об остатках.

**4.15. Выводы.**

## ГЛАВА 5. ПОСЛЕДНЯЯ ТЕОРЕМА ФЕРМА ДЛЯ РЕГУЛЯРНЫХ ПРОСТЫХ . . . . .

182

**5.1. Замечания Куммера о квадратичных целых.** Понятие эквивалентности дивизоров. Упоминание Куммером теории дивизоров для квадратичных целых  $x + y\sqrt{D}$  и связь ее с гауссовой теорией бинарных квадратичных форм.

**5.2. Эквивалентность дивизоров в частном случае.** Изучение вопроса: какие дивизоры являются дивизорами круговых целых? — в частном случае.

**5.3. Число классов.** Определение и основные свойства эквивалентности дивизоров. Системы представителей. Доказательство конечности числа классов.

**5.4. Два условия Куммера.** Характер аргументации, использованной в доказательствах Последней теоремы Ферма для показателей 3 и 5, обуславливает выделение среди простых чисел  $\lambda$  тех, для которых (A) число классов не делится на  $\lambda$  и (B) единицы, сравнимые по модулю  $\lambda$  с целыми числами, являются  $\lambda$ -ми степенями. Такие простые названы регулярными.

**5.5. Доказательство для регулярных простых.** Куммеров вывод Последней теоремы Ферма для регулярных простых показателей. Для любой единицы  $e(\alpha)$  единица  $e(\alpha)/e(\alpha^{-1})$  имеет вид  $\alpha^r$ .

**5.6. Квадратичная взаимность.** Теория Куммера ведет не только к доказательству знаменитого квадратичного закона взаимности, но и к выводу формулировки этого закона. Символы Лежандра. Дополнительные законы.

## ГЛАВА 6. ОПРЕДЕЛЕНИЕ ЧИСЛА КЛАССОВ . . . . .

216

**6.1. Введение.** Основная теорема, которую нужно доказать, — это теорема Куммера о том, что число  $\lambda$  тогда и только тогда регулярно, когда оно делит числители чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$ .

**6.2. Формула эйлера произведения.** Аналог формулы для случая круговых целых. Формула числа классов находится умножением обеих частей на  $(s - 1)$  и вычислением предела при  $s \downarrow 1$ .

**6.3. Первые шаги.** Доказательство обобщенной формулы эйлера произведения. Дзета-функция Римана.

**6.4. Преобразование правой части.** Правая часть равна  $\zeta(s) L(s, \chi_1) L(s, \chi_2) \dots L(s, \chi_{\lambda-2})$ , где  $\chi_i$  — неглавные характеры по модулю  $\lambda$ .

**6.5. Проведенное Дирихле вычисление значений  $L(1, \chi)$ .** Суммирование по частям.  $L(1, \chi)$  как суперпозиция рядов для  $\log(1/(1 - \alpha^j))$ ,  $j = 1, 2, \dots, \lambda - 1$ . Явная формула для  $L(1, \chi)$ .

**6.6. Предел правой части.** Явная формула.

**6.7. Необращение в нуль  $L$ -рядов.** Дока-

зательство того, что  $L(1, \chi) \neq 0$  для рассматриваемых характеров  $\chi$ . **6.8. Преобразование левой части.** Предел при  $s \downarrow 1$  суммы слагаемых  $N(A)^{-s}$  по всем дивизорам  $A$  из класса дивизоров одинаков для любых двух классов. Программа вычисления общего предела таких сумм. **6.9. Единицы: несколько первых случаев.** Явное извлечение всех единиц в случаях  $\lambda = 3, 5, 7$ . Конечномерный анализ Фурье. Неявное извлечение единиц в случае  $\lambda = 11$ . Второй сомножитель числа классов. **6.11. Единицы: общий случай.** Метод нахождения (по крайней мере в принципе) всех единиц. Сумма по всем главным дивизорам, записанная как сумма по некоторому множеству круговых целых. **6.10. Вычисление интеграла.** Решение одной задачи интегрального исчисления. **6.12. Сравнение интеграла с суммой.** В вычисляемом пределе сумма может быть заменена интегралом. **6.13. Сумма по другим классам дивизоров.** Доказательство того, что в пределе сумма по любым двум классам дивизоров одна и та же. **6.14. Формула числа классов.** Объединение всех частей, разбросанных в предшествующих параграфах, и получение явной формулы числа классов. **6.15. Доказательство иррегулярности числа 37.** Упрощение подсчета первого сомножителя числа классов. Числа Бернулли и полиномы Бернулли. **6.16. Делимость первого сомножителя на  $\lambda$ .** Обобщение техники предыдущего параграфа с тем, чтобы показать, что число  $\lambda$  тогда и только тогда делит первый сомножитель числа классов, когда оно делит числитель одного из чисел Бернулли  $B_2, B_4, \dots, B_{\lambda-3}$ . **6.17. Делимость второго сомножителя на  $\lambda$ .** Доказательство того, что  $\lambda$  только тогда делит второй сомножитель, когда оно делит также и первый сомножитель. **6.18. Лемма Куммера.** Из (A) вытекает (B). **6.19. Краткие выводы.**

## ГЛАВА 7. ТЕОРИЯ ДИВИЗОРОВ КВАДРАТИЧНЫХ ЦЕЛЫХ 290

**7.1. Простые дивизоры.** Чем должны быть простые дивизоры, если мы хотим, чтобы существовала теория дивизоров для чисел вида  $x + y\sqrt{D}$ . Модификация определения квадратичных целых при  $D \equiv 1 \pmod{4}$ . **7.2. Теория дивизоров.** Доказывается, что определенные в предыдущем параграфе дивизоры дают теорию дивизоров со всеми ожидаемыми свойствами. Эквивалентность дивизоров. **7.3. Знак нормы.** При  $D > 0$  норма принимает как положительные, так и отрицательные значения. В этом случае вводится дивизор с нормой  $-1$ . **7.4. Квадратичные целые с данными дивизорами.** В отличие от кругового случая для квадратичных целых существует простой алгоритм, позволяющий определить, является ли данный дивизор главным, и, если это так, найти все квадратичные целые с данным дивизором. По существу, этот алгоритм совпадает с циклическим методом древних индийцев. Обоснование алгоритма при  $D < 0$ . Упражнения: использование  $2 \times 2$ -матриц для сокращения вычислений циклического метода. **7.5. Обоснование циклического метода.** Доказательство в случае  $D > 0$ . Вычисление основной единицы. **7.6. Группа классов дивизоров: примеры.** Явное нахождение группы классов дивизоров для нескольких значений  $D$ . **7.7. Группа классов дивизоров: общая теорема.** Доказывается, что два дивизора эквивалентны только тогда, когда применение к ним циклического метода дает один и тот же период приведенных дивизоров. Это упрощает нахождение группы классов дивизоров. **7.8. Теоремы Эйлера.** Эйлер эмпирически обнаружил, что закон разложения простого числа  $p$  в квадратичных целых  $x + y\sqrt{D}$  зависит только от класса  $p$  по модулю  $4D$ . Он

открыл также другие теоремы, которые упрощают нахождение тех классов простых по модулю  $4D$ , которые содержат распадающиеся простые или простые, остающиеся простыми при переходе к квадратичным целым детерминанта  $D$ . Эти теоремы (не доказанные Эйлером) равносильны квадратичному закону взаимности. **7.9. Роды классов дивизоров.** Необходимые условия Гаусса для эквивалентности двух дивизоров. Характер класса дивизоров. Возникающее при этом разбиение группы классов дивизоров на роды. **7.10. Двусторонние классы.** Определение. Доказывается, что число двусторонних классов не превосходит половины числа возможных характеров. **7.11. Второе доказательство Гаусса квадратичного закона взаимности.** Доказывается, что в действительности встречается не более половины возможных характеров. Из этой теоремы Гаусс выводит квадратичный закон взаимности.

## ГЛАВА 8. ГАУССОВА ТЕОРИЯ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ . . . . . 363

**8.1. Другие группы классов дивизоров.** Если  $D$  не свободно от квадратов, то требуется изменить определение группы классов дивизоров. Порядки квадратичных целых. Эквивалентность относительно порядка. Группа классов дивизоров, соответствующих порядку. Упражнения: удобные числа Эйлера. **8.2. Другая интерпретация циклического метода.** Интерпретация циклического метода как метода порождения эквивалентных бинарных квадратичных форм. Метод нахождения представлений данных целых чисел данными бинарными квадратичными формами. **8.3. Соответствие между дивизорами и бинарными квадратичными формами.** Собственная эквивалентность бинарных квадратичных форм. Взаимно однозначное соответствие между классами собственной эквивалентности собственно примитивных форм (положительных при  $D > 0$ ) и классами дивизоров порядка  $\{x + y \sqrt{D} : x, y \text{ — целые}\}$ . **8.4. Классификация форм.** Распространение теоремы из § 7.7 на случай не свободного от квадратов  $D$ . **8.5. Примеры.** Нахождение группы классов дивизоров в нескольких случаях. **8.6. Гауссова композиция форм.** Как Гаусс определил произведение двух классов бинарных квадратичных форм, не используя теории дивизоров. **8.7. Уравнения второй степени с двумя неизвестными.** Полное решение (по существу, принадлежащее Лагранжу) уравнения  $ax^2 + bxy + cy^2 + dx + ey + f = 0$ .

## ГЛАВА 9. ФОРМУЛА ДИРИХЛЕ ДЛЯ ЧИСЛА КЛАССОВ . . . . . 406

**9.1. Формула эйлера произведения.** Аналог этой формулы для квадратичных целых. Разбиение на случаи для различных типов  $D$ . **9.2. Первый случай.** Случай  $D < 0$ ,  $D \not\equiv 1 \pmod{4}$ ,  $D$  свободно от квадратов. Вывод формулы числа классов. Примеры. **9.7. Второй случай.** Случай  $D > 0$ ,  $D \not\equiv 1 \pmod{4}$ ,  $D$  свободно от квадратов. Вывод. Примеры. **9.4. Случай  $D \equiv 1 \pmod{4}$ .** Изменения, которые требуются при  $D \equiv 1 \pmod{4}$ ,  $D$  свободно от квадратов. **9.5. Вычисление суммы  $\sum \binom{D}{n} \frac{1}{n}$ .** Эту часть формулы числа классов можно подсчитать методами § 6.5. Преобразование Фурье характера  $\binom{D}{n}$  по модулю  $4D$  кратно самому характеру. Этот факт используется для редукции формулы. Упражнения: дальнейшие упрощения Дирихле формулы числа классов при  $D < 0$ ,  $D$  свободно от квадратов. Знак гауссовой суммы и его связь с формулой Дирихле.

9.6. Подпорядки. Обобщение формулы числа классов на случай не свободного от квадратов  $D$  и, вообще, на случай групп классов дивизоров, соответствующих произвольным порядкам квадратичных целых. 9.7. Простые в арифметических прогрессиях. Приводится доказательство Дирихле теоремы о том, что формула  $an + b$  при  $b$ , взаимно простом с  $a$ , дает бесконечно много простых чисел. Формула числа классов используется при доказательстве неравенства  $L(1, \chi) \neq 0$  для всех вещественных характеров  $\chi$  по модулю  $a$ .

ПРИЛОЖЕНИЕ. НАТУРАЛЬНЫЕ ЧИСЛА . . . . .	439
---	-----

А.1. Основные свойства. Сложение и умножение. Алгоритм Евклида. Сравнение по модулю натурального числа. Китайская теорема об остатках. Решение сравнения  $ax \equiv b \pmod c$ . Основная теорема арифметики. Целые числа. А.2. Примитивные корни по модулю  $p$ . Определение. Доказательство того, что каждое  $p$  имеет примитивный корень.

Ответы к упражнениям . . . . .	448
Литература . . . . .	472
Указатель . . . . .	477



# УВАЖАЕМЫЙ ЧИТАТЕЛЬ!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присылать по адресу: 129820, Москва, И-110, ГСП, 1-й Рижский пер., д. 2, издательство «Мир».

---

Г. Эдвардс

**ПОСЛЕДНЯЯ ТЕОРЕМА ФЕРМА  
ГЕНЕТИЧЕСКОЕ ВВЕДЕНИЕ В АЛГЕБРАИЧЕСКУЮ  
ТЕОРИЮ ЧИСЕЛ**

Ст. научный редактор Н. И. Плужникова  
Мл. научный редактор Ю. С. Андреева  
Художник Н. Ф. Алексеев  
Художественный редактор В. И. Шаповалов  
Технический редактор Г. Б. Алюлина  
Корректор Н. И. Баранова

ИБ № 1943

Сдано в набор 24.06.80.  
Подписано к печати 20.10.80.  
Формат 60×90<sup>1/16</sup>.  
Бумага типографская № 1.  
Гарнитура обыкновенная. Печать высокая.  
Объем 15,25 бум. л. Усл. печ. л. 30,5.  
Уч.-изд. л. 32.06, Изд. № 1/0294.  
Тираж 8000 экз. Зак. 0876. Цена 3 р.

**ИЗДАТЕЛЬСТВО «МИР»**  
Москва, 1-й Рижский пер., 2.

Ордена Трудового Красного Знамени  
Московская типография № 7 «Искра революции» Союзполиграфпрома  
Государственного Комитета СССР по делам издательств,  
полиграфии и книжной торговли.  
Москва 103001, Трехпрудный пер., 9.



Г. Эдвардс

# ПОСЛЕДНЯЯ ТЕОРЕМА ФЕРМА

Генетическое введение  
В АЛГЕБРАИЧЕСКУЮ  
ТЕОРИЮ ЧИСЕЛ